**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF VIRGINIA**
**Alexandria Division**

| | |
|---|---|
| *In re Capital One Financial Corporation, Affiliate Marketing Litigation* | Civil Action No. 1:25-cv-00023-AJT-WBP<br><br>**AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

Plaintiffs Ahntourage Media LLC, Just Josh, Inc., Storm Productions LLC, TechSource Official, and ToastyBros, LLC, on behalf of themselves and all others similarly situated, bring this action against Defendants Capital One Financial Corporation, Wikibuy, LLC, and Wikibuy Holdings, LLC, (together, "Capital One") and allege as follows:

## I. INTRODUCTION

1. The Capital One Shopping browser extension is a free tool with over ten million users that claims to help online shoppers search for coupons, find better prices, and earn rewards redeemable for gift cards. But behind this facade, the Capital One Shopping browser extension steals commissions from bloggers, YouTubers, website operators, online publications, influencers, and other creators who drive online sales.

2. Plaintiffs are creators that earn these commissions by promoting products and services to their audiences through affiliate links shared on their platforms and social media channels. These links, provided by online merchants and third-party affiliate marketing platforms, contain unique affiliate tracking codes—such as cookies, tracking tags, or server-side functions—that identify the creator. When a consumer clicks an affiliate link and makes a purchase, the merchant or affiliate marketing platform uses that tracking code to credit the creator with the referral and ensure that the creator receives a commission on the sale.

3. The Capital One Shopping browser extension, however, exploits this attribution

system to systematically misappropriate creators' commissions. During the checkout process, the Capital One Shopping browser extension artificially simulates a referral click by the consumer, making it appear that the purchase occurred after the purchaser navigated to the merchant's site by clicking on a Capital One affiliate link. In reality, the purchaser was already on the merchant's site and neither saw nor clicked any Capital One referral links. This simulated referral click enables Capital One to displace the creator's affiliate tracking code and insert Capital One's own tracking code in its place—even though the consumer used the creator's specific affiliate link, not Capital One's, to visit the merchant's website and make a purchase. The result: Capital One takes the commission, leaving the creator who did the work to drive the purchase empty-handed.

4. Plaintiffs bring this class action on their own behalf and on behalf of all other creators similarly situated to recover the damages they have sustained and enjoin Capital One's wrongful conduct.

## II. JURISDICTION

5. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is diverse in citizenship from Capital One, there are at least 100 Class members nationwide, and the aggregate amount in controversy exceeds $5,000,000. This Court also has jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1367.

6. This Court has personal jurisdiction over Capital One because Capital One is headquartered in McLean, Virginia, does business in Virginia, directly or through agents, and has sufficient minimum contacts with Virginia such that it has intentionally availed itself of the state's laws.

7. Venue is proper under 28 U.S.C. § 1391(a) through (d) because Capital One's headquarters and principal place of business are located in this judicial district, Capital One resides

in this district, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this district, including, without limitation, decisions made by Capital One's governance and management personnel.

## III. PARTIES

### A. Plaintiffs

8. Ahntourage Media LLC ("Ahntourage Media") is an S corporation organized and existing under the laws of Pennsylvania, with its principal place of business in Trevose, Pennsylvania.

9. Just Josh, Inc., ("Just Josh") is an S corporation organized and existing under the laws of Arizona, with its principal place of business in Scottsdale, Arizona.

10. Storm Productions LLC ("Madison Avenue Spy") is a limited liability company organized and existing under the laws of New York, with its principal place of business in New York, New York.

11. TechSource Official ("TechSource") is an S corporation organized and existing under the laws of California, with its principal place of business in Sacramento, California.

12. ToastyBros, LLC, ("ToastyBros") is a limited liability company organized and existing under the laws of Kentucky, with its principal place of business in Louisville, Kentucky.

### B. Defendants

13. Capital One Financial Corporation is a corporation incorporated in Delaware, with its headquarters and principal place of business in McLean, Virginia.

14. Wikibuy, LLC, and Wikibuy Holdings, LLC, are subsidiaries of Capital One Financial Corporation organized and existing under the laws of Delaware that originally developed the Capital One Shopping browser extension.

15. Capital One Financial Corporation, Wikibuy, LLC, and Wikibuy Holdings, LLC, are collectively referred to herein as "Capital One."

16. Capital One transacts business and is headquartered within this judicial district, specifically at 1680 Capital One Drive, McLean, Virginia 22102-3491.

## IV. FACTUAL ALLEGATIONS

### A. Background

#### 1. The Capital One Shopping Browser Extension

17. In late 2018, Capital One acquired, for an undisclosed amount, an online-shopping startup behind a browser extension called WikiBuy, which allowed consumers to compare product prices when shopping online.[1] Capital One later rebranded the extension, calling it Capital One Shopping.

18. Capital One markets the Capital One Shopping browser extension as a free tool that helps consumers save time and money while shopping online. The extension is available to everyone; a consumer need not be a Capital One customer to use it. Capital One Shopping currently boasts over 10 million users.

19. Consumers can use Capital One Shopping on desktop and laptop computers by downloading the browser extension from their web browser's extension store. Consumers can also use Capital One Shopping on mobile devices by downloading the Capital One Shopping mobile application from the Apple App Store or Google Play Store.

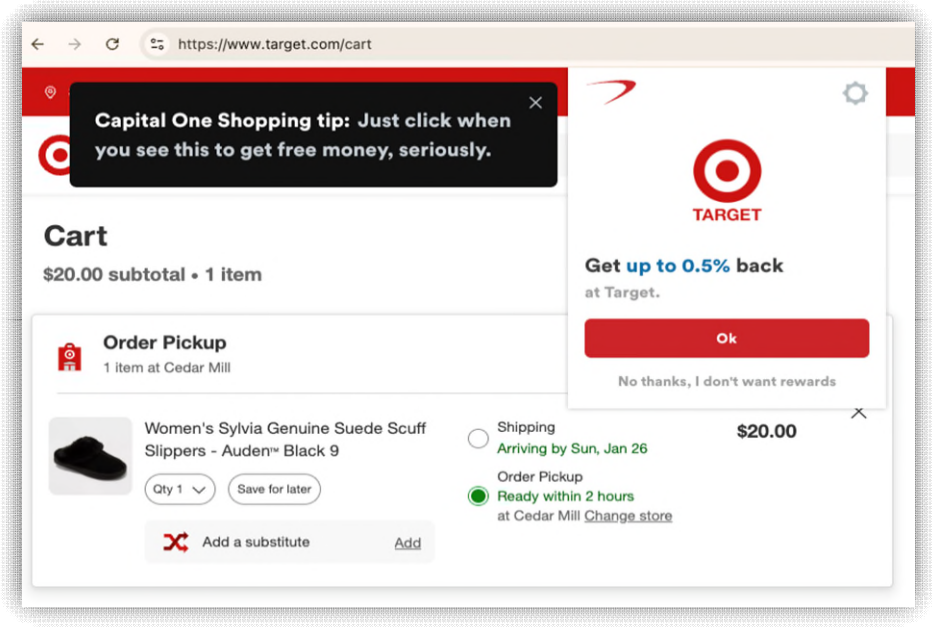
20. Capital One entices consumers to download the Capital One Shopping browser

[1] A browser extension is a small piece of software that adds features to a web browser or to programs used in a browser. *Everything to Know About Browser Extensions*, Microsoft (Mar. 6, 2023), https://www.microsoft.com/en-us/edge/learning-center/everything-to-know-about-browserextensions?form=MA13I2.

extension by promising to test and apply available discount, promotional, and coupon codes to items already in consumers' online shopping carts.

21. Capital One also entices consumers to download and use the Capital One Shopping browser extension by offering price-comparison tools and cash-back rewards redeemable for gift cards from popular merchants.

22. Even when the Capital One Shopping browser extension cannot find a working coupon code for a product or service offered by an online merchant partner, a Capital One Shopping pop-up may still appear purporting to offer possible rewards for consumers making eligible purchases:




23. Once installed, the Capital One Shopping browser extension operates on all webpages that a consumer visits. It continuously reads and collects a massive trove of data from the consumer as that consumer navigates the web—regardless of whether the consumer engages with the extension. In other words, even absent any direct or purposeful interaction by the consumer with the extension's interface, functionality, or features, the extension still runs in the

background on every webpage visited by the consumer, gathering constant data about that consumer's online activity.

24. The Capital One Shopping browser extension works on over 100,000 online merchants' websites, including Best Buy, Herman Miller, Mytheresa, Net-a-Porter, Newegg, Macy's, Walmart, Staples, and Target.[2]

25. Capital One Shopping earns considerable revenue through commissions obtained from its merchant partners.[3]

26. Capital One lists Capital One Shopping as one of its sources of non-interest income. According to Capital One's annual report for 2023, the company earned $7.5 billion in non-interest income, including income from Capital One Shopping.[4]

**2. Affiliate Marketing: Partnerships Between Merchants and Creators**

27. Affiliate marketing is a multi-billion-dollar industry built on partnerships between online merchants and creators. As e-commerce and platforms like YouTube, Instagram, and TikTok have surged in popularity, merchants have increasingly turned to creators to promote their products and services—leveraging the trust and influence that the creators have built with their audiences.

28. Through affiliate-marketing programs, online merchants enable creators to promote their products and services in exchange for commissions on resulting sales. Merchants may manage these programs directly or use affiliate-marketing platforms like Impact, Rakuten, and CJ

[2] Capital One, *Capital One Shopping*, https://www.capitalone.com/learn-grow/money-management/capital-one-shopping/ (last visited Mar. 21, 2025).
[3] Capital One Shopping, *United States Terms of Service*, https://capitaloneshopping.com/our-terms/terms-of-service (last visited Feb. 4, 2025).
[4] Capital One, Annual Report 2023 at 57 (2023), https://ir-capitalone.gcs-web.com/static-files/3381e479-cf44-4a85-a0f6-b7d8d30c2a31.

Affiliate, which are third-party intermediaries that connect merchants with creators and manage their partnerships.

29. Creators earn commissions by directing their audiences to merchants' products and services via affiliate links that they share on their various platforms and social media channels.

**3. The Affiliate Link Attribution System**

30. Affiliate links are web-based hyperlinks that direct consumers to a website where they can purchase the product or service being promoted by a creator.

31. Online merchants use affiliate tracking codes—like cookies, tracking tags, or server-side functions—to determine whether a consumer landed on the webpage for their product or service and made a purchase after having clicked an affiliate link. Merchants thereby attribute the sale to the creator responsible for the affiliate link and provide a commission to that creator.

32. More specifically, affiliate marketing generally works as follows:[5]

a. **First**, a creator will partner with an online merchant to promote its products and services. Often, this partnership is facilitated through an affiliate network, a third party that connects creators and online merchants and sometimes manages the partnership. As part of the partnership, an online merchant will provide an "affiliate link" to the creator. An affiliate link is a unique URL associated only with that specific creator. When a consumer clicks on the creator's affiliate link, the link redirects the consumer to the webpage of the product or service that the online merchant is selling and the creator is promoting.

b. **Second**, a creator creates marketing "content," promoting an online merchant's

[5] GRIN Contributor, *Affiliate Marketing for Beginners in 2024*, GRIN, https://grin.co/blog/affiliate-marketing-for-beginners/ (last visited Feb. 4, 2025).

product or service. Examples of "content" include websites, blog posts, videos on YouTube and TikTok, Instagram and Facebook posts and stories, live streams on Twitch, and text posts on X (formerly Twitter). The creator will include the affiliate link with their content.

c. **Third**, a creator will post or stream affiliate content on their website, social media account, and other online locations. Third parties who view that content have access to the affiliate link.

d. **Fourth**, a consumer viewing the creator's content uses the affiliate link (by clicking on the link directly or by copying the link into their browser's search bar) to view the online merchant's webpage for the product or service that the creator was promoting. The viewer then purchases the promoted product or service.

e. **Fifth**, because the consumer purchased the online merchant's product or service after using the affiliate link to navigate to the merchant's site, the online merchant provides the creator with a commission for the sale of the product or service. The commission rate that a creator will receive varies depending on the merchant, product, or service being promoted. For example, the breakdown of average commission rates by product category in 2022-2023 was:[6]

[6] Refersion, *How to Negotiate with Affiliates* (Mar. 1, 2023), https://www.refersion.com/blog/affiliates-negotiation/#:~:text=If%20they're%20underperforming%2C%20then,be%20time%20for%20a%20bonus.

| Product Category | Affiliate Commissions (% of Sale) |
|---|---|
| Arts & Crafts | 12% |
| Beauty | 15-20% |
| Business | 20-25% |
| Clothing | 10-15% |
| Computers & Tech | 15-20% |
| Education | 20% |
| Family | 20-25% |
| Financial | 30-40% |
| Fitness | 10-20% |
| Food & Drink | 10-20% |
| Hair | 10% |
| Health | 20-30%+ |
| Home | 10-20% |
| Jewelry | 15-30% |
| Paleo | 10% |
| Pets | 10-20% |
| General Products | 10-20% |
| Recreation | 10% |
| Services | 30% |
| SaaS | 20-30% |
| Adult | 10-15%+ |

33. Around 80% of creators earn $80,000 or less per year from affiliate marketing, while top creators can take in over $1 million per year:[7]

| Income | Share of Affiliate Marketers |
|---|---|
| Up to $80,000 | 80% |
| $80,000 to $1 Million | 15% |
| Over $1 Million | 1% |

34. In 2023, the affiliate marketing industry generated $15.7 billion in revenue and, according to a report by Astute Analytica, its revenue is expected to grow to $36.9 billion by 2030.[8]

35. The affiliate marketing industry is profitable because it is an effective way to

[7] Shubham Singh, *113 Affiliate Marketing Statistics (2025): Market Size & Trends*, demandsage (Dec. 27, 2024), https://www.demandsage.com/affiliate-marketing-statistics/.

[8] Rewardful Team, *18 Affiliate Marketing Statistics for 2025*, Rewardful (Dec. 5, 2024), https://www.rewardful.com/articles/affiliate-marketing-statistics#:~:text=The%20affiliate%20marketing%20market%20size,reach%20%2415.7%20billion%20by%202024.

market products and services to consumers.

36. According to the 2024 Modern Consumer Survey published by GRIN, the world's leading online creator management platform, 74% of consumers have purchased a product because a social media influencer has recommended it.[9]

37. In a 2023 survey from Matter Communications, 69% of survey respondents were more likely to trust a creator's recommendation of a product or service over information that an online merchant had provided about its product or service.[10]

38. Affiliate marketing currently results in 16% of all e-commerce sales in the United States.[11]

**4. How Affiliate Links Work and the Last-Click Attribution Model**

39. An affiliate link is a custom URL assigned to a creator by an online merchant.[12] The URL includes the creator's "affiliate ID," which is a specialized number or username that allows the online merchant to identify the affiliate involved in the sale.[13] The affiliate link thus allows an online merchant to credit a particular creator with commissions for any sales of the online merchant's products or services that result from that creator's marketing efforts.[14]

---

[9] GRIN, *U.S. Shoppers Are Under the Influence: 74% of Consumers Have Purchased a Product Because an Influencer Recommended It*, BusinessWire (Mar. 20, 2024, 8:00 AM) https://www.businesswire.com/news/home/20240320786326/en/U.S.-Shoppers-Are-Under-the-Influence-74-of-Consumers-Have-Purchased-a-Product-Because-an-Influencer-Recommended-It.

[10] Elise Dopson, *28 Important Influencer Marketing Statistics To Know in 2025*, Shopify (Nov. 11, 2024) https://www.shopify.com/blog/influencer-marketing-statistics.

[11] Arya Bina, *How Affiliate Networks Have Taken Affiliate Marketing Mainstream*, Forbes (Apr. 21, 2017, 7:00 AM) https://www.forbes.com/sites/forbesagencycouncil/2017/04/21/how-affiliate-networks-have-taken-affiliate-marketing-mainstream/?sh=5cdbd827569d.

[12] Dibakar Ghosh, *What Are Affiliate Links and How Do They Work?*, AuthorityHacker (Aug. 12, 2024) https://www.authorityhacker.com/what-are-affiliate-links/.

[13] *Id.*

[14] *Id.*

40. While affiliate links vary in appearance, the URL for those links generally contain the following common elements:[15]


41. When a creator promotes an online merchant's product or service and shares the affiliate link for that product or service, a consumer viewing the creator's content can click on the affiliate link and be directed to a webpage on which the online merchant is selling the promoted product or service.[16]

42. When the consumer clicks the affiliate link, a small text file is often stored on that consumer's web browser that includes information about the creator who provided the consumer with the affiliate link.[17] The small text file is called a "cookie." Affiliate attribution tracking occurs predominantly through the use of cookies, but it can also occur through server-side functions or tracking tags embedded directly in a URL.[18]

43. Once a cookie is stored on a consumer's web browser, the cookie tracks the consumer's activity on the online merchant's website to determine whether the consumer ultimately purchased a product or service.[19]

---

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] For the sake of simplicity, and due to the prevalence of cookies as a mechanism for affiliate attribution tracking, this section delves deeper into the technical functionality of cookies in the affiliate context. Other mechanisms of affiliate attribution tracking, while not discussed in detail in the complaint, work analogously and aim to achieve the same end: awarding commission to the creator of the affiliate link credited with referring a sale to a given merchant.
[19] *Id.*

44. A cookie associated with an affiliate link can be stored on a consumer's web browser from anywhere from 24 hours to 90 days or longer, with the cookie's lifespan determined by the online merchant that created the affiliate link for the creator.[20] By endowing a cookie with a longer lifespan, a merchant allows for the following series of events: if a consumer clicks on an affiliate link to view the product or service that a creator has promoted, closes out of the online merchant's webpage for that product or service for whatever reason, but then returns to the online merchant's website later to ultimately purchase the product or service, the creator can still be rewarded with the commission from the sale.[21]

45. This cookie-tracking process can, however, be disrupted. For example, if a consumer clicks on affiliate links from different creators that direct the consumer to the same merchants' webpage, the online merchant will only provide a commission for the sale of the product or service to the creator associated with the last-used affiliate link of the purchaser—the "last-click" convention discussed above. This is called the "last-click attribution model,"[22] and it is the predominant model for awarding affiliate commissions on the internet today.

46. Last-click attribution is a "single-touch" attribution model that gives all credit for a purchase to the final touchpoint in a consumer's journey that leads the consumer to merchant's page where the consumer will ultimately complete a purchase.

47. According to the Interactive Advertising Bureau's[23] Digital Attribution Primer 2.0, a "click" is defined as "the measurement of navigating from one page to another by activating a

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] The Interactive Advertising Bureau is an American advertising business organization that develops industry standards, conducts research, and provides legal support for the online advertising industry.

hyperlink."[24] In other words, a "click" under this model refers to a consumer's interaction with a digital ad or other online content, such as clicking on a link, button, or image, that *leads* the consumer to a merchant's specific website or landing page from which the consumer can complete the purchase.[25] This interaction can also occur when a consumer copies a hyperlink into the URL bar directly to navigate to the merchant's page. To be clear: "last click" refers to the last link clicked that directed the consumer to the merchant's website.

48. "Last click" is *not* defined as an action the consumer takes once the consumer has already landed on the merchant's site. In other words, "last click" does not literally mean "last click made before consumer purchases." This is self-evidently true given that to make a purchase the consumer has to click on a variety of buttons on the merchant's own website—such as the merchant's link for the product, color/size specifications, links to enter payment and delivery information, and the purchase link—and yet the merchant does not count those as the "last click" for the purpose of referral attribution and the awarding of commissions.

49. "Last click" is also *not* defined as other clicks the consumer makes on their own computer prior to making a purchase, even if those clicks may have contributed to the consumer's purchasing decision. For example, a consumer may have two tabs open simultaneously, one for a merchant whose site the consumer navigated to using an affiliate link, and one for a product review site. The consumer may put an item in their cart on the merchant site, and then click on the product review site to learn more about the product before purchasing it. If the consumer does not use the product review site to *navigate to* the merchant's site, the product review site is not entitled to a commission even though the consumer's "last click" may have been on that site.

[24] https://www.iab.com/wp-content/uploads/2016/10/Digital-Attribution-Primer-2-0-FINAL.pdf

[25]

**5. Applicable Commission Attribution Rules**

50. Plaintiffs and Class members have entered into contractual agreements with Capital One's merchant partners that are consistent with the last-click attribution model described above. Pursuant to these contracts, Plaintiffs and Class members are entitled to commissions when a consumer's final external click before entering a merchant's website and making a qualifying purchase was a click on the creator's affiliate link.

51. For example, Madison Avenue Spy's and Class members' agreements with Capital One merchant partner Zadig & Voltaire specify that they will earn a commission "once a user conducts a Qualifying Action using the Qualifying Link displayed from Your digital property." A "Qualifying Action" is defined as a "purchase of a product, completion or fulfillment of an application or other action by a user required by Us for a commission."

52. Similarly, ToastyBros' and Class members' agreements with Capital One merchant partner AliExpress specify that they will earn a commission for "every Qualifying Purchase by a Buyer on the AliExpress Platform which can be validly attributed to or traced to have originated from an advertisement published, displayed, disseminated and/or distributed by Participant and/or Participant's Advertising Channel, such Participant shall be entitled to claim a commission from AliExpress." The AliExpress agreement explains that the "Transaction Price" for commissions for "Qualifying Purchases" specifically excludes, for example, "discounts" and "coupons."

53. Just Josh's, ToastyBros', and Class members' agreements with Capital One merchant partner Best Buy specify that Class members will earn commissions on qualifying purchases that are "made via the intentional click by a Customer of a Qualifying Link that can be tracked and reported on through the use of Impact's tracking technology and/or methodology during an active Session." Impact is an affiliate marketing platform and can track and report on

creators' affiliate links, including the last referral click the consumer made prior to the Capital One Shopping browser extension replacing that link.

54. Just Josh's, ToastyBros', and Class members' agreements with Capital One merchant partner Walmart provide that they will earn commissions "on products that are actually purchased by a customer within the relevant cookie window after the customer has initially entered [the Walmart] Site as long as the customer re-enters [the] Site directly during that time and not through another affiliate link." These agreements also expressly prohibit Capital One's method of engaging in commission theft. Specifically, the agreements explain that the "use [of] any type of method, software, automated script, or technology which attempts to intercept or redirect traffic or Commissions to or from any website, or otherwise artificially increase Commissions" is strictly prohibited. The agreements further advise directly that the affiliate party may not "employ, use, or receive any direct or indirect benefit from, any 'cookie stuffing' methods (e.g., use of 'cookie stuffing' to cause the Platform's tracking systems to conclude that a user has clicked through a Qualifying Link - and to pay Commissions accordingly - even if the user has not actually clicked through any such link)."

55. Ahntourage's and Class members' agreements with Capital One merchant partner Staples states that "[s]ales generated through the Affiliate link entitle the Affiliate to earn a cash commission" and that Staples "will fund payment for all commissions due to [the Affiliate]."

56. Similarly, Madison Spy Avenue's and Class members' agreements with Capital One merchant partner Gap-Old Navy provide that product sales "will qualify for a commission when," in relevant part, the "products are purchased by users linking to the Gap Inc. Site(s) for which Your Site is an Affiliate, from Your Site through a Link." These agreements also expressly prohibit Capital One's conduct. Specifically, the agreements explain that "Your Site may not

contain software or use technology that attempts to intercept, divert or redirect Internet traffic to or from any other website, or that potentially enables the diversion of Affiliate commissions from another website. This includes toolbars, browser plug-ins, extensions and add-ons."

57. Madison Avenue Spy's and Class members' agreements with Capital One merchant partner Target provide that they are entitled to commissions "on sales of Qualifying Products or Qualifying Actions" if the consumer "use[s] a browser that has its cookies setting enabled" and "follow[s] a Qualifying Link." A "Qualifying Link" is "any type of banner or text link provided by Target to be displayed, distributed[,] or played on your site or Affiliate Materials and can be tracked through Target's Target Vendor." Target also expressly prohibits Capital One's conduct. Specifically, Target's agreements with Class members explain that "[a] site or Affiliate Materials may be found unsuitable if they . . . [c]ontain software or use technology that attempts to intercept, divert or redirect Internet traffic to or from any other website, or that potentially enables the diversion of affiliate commissions from another website."

58. Thus, both under the prevailing last-click attribution model and creators' express agreements with merchants, creators are entitled to commissions when the creator's affiliate link was a consumer's final click *external* to the merchant's webpage—a click that directed the consumer to the merchant's webpage on which the consumer completed a qualifying purchase.

59. For example, Plaintiff Madison Avenue Spy promotes goods sold by a merchant called Mytheresa. When a buyer[26] navigates to Mytheresa's webpage by clicking an affiliate link shared by Madison Avenue Spy and completes a purchase, Madison Avenue Spy is entitled to receive a commission for the sale.

[26] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

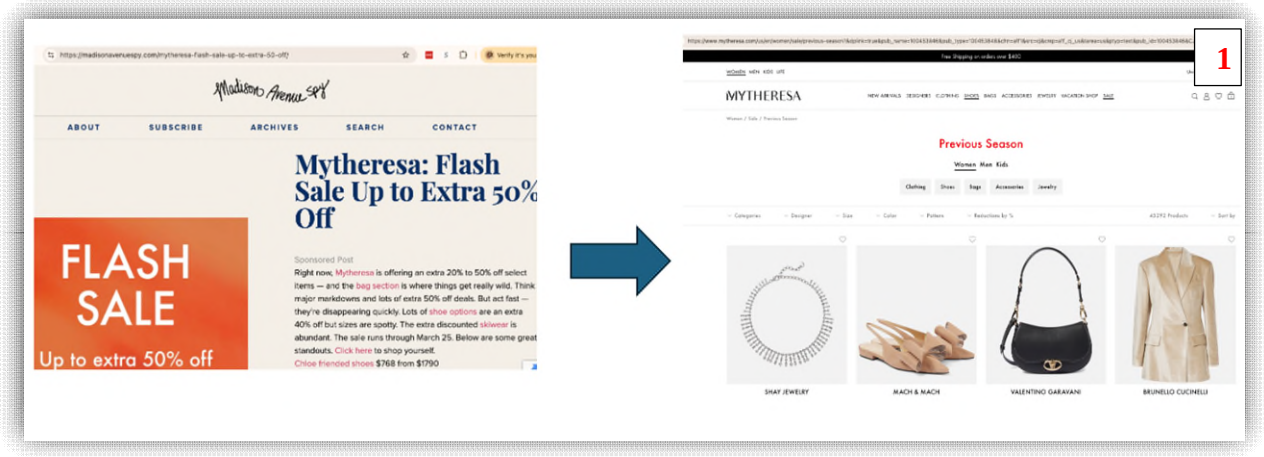



Image 1: A buyer navigates to a Mytheresa's webpage by clicking an affiliate link shared by Plaintiff Madison Avenue Spy on her fashion blog Madison Avenue Spy.

60. When the buyer lands on the Mytheresa webpage after clicking Madison Avenue Spy's affiliate link, the browser stores a cookie identifying Madison Avenue Spy as the "referrer" of the buyer to the webpage.

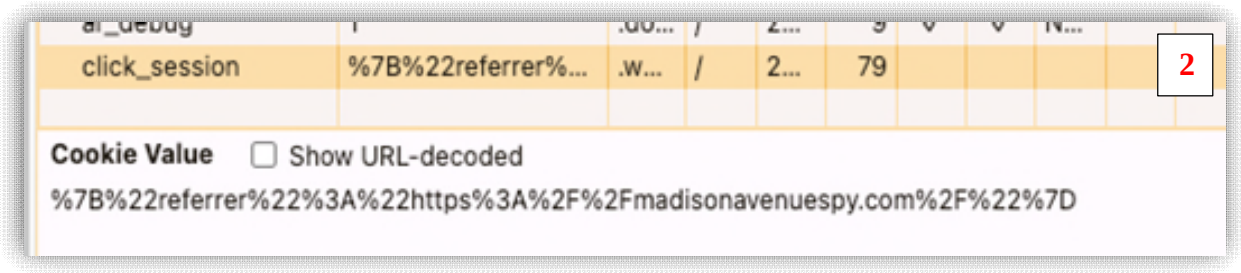
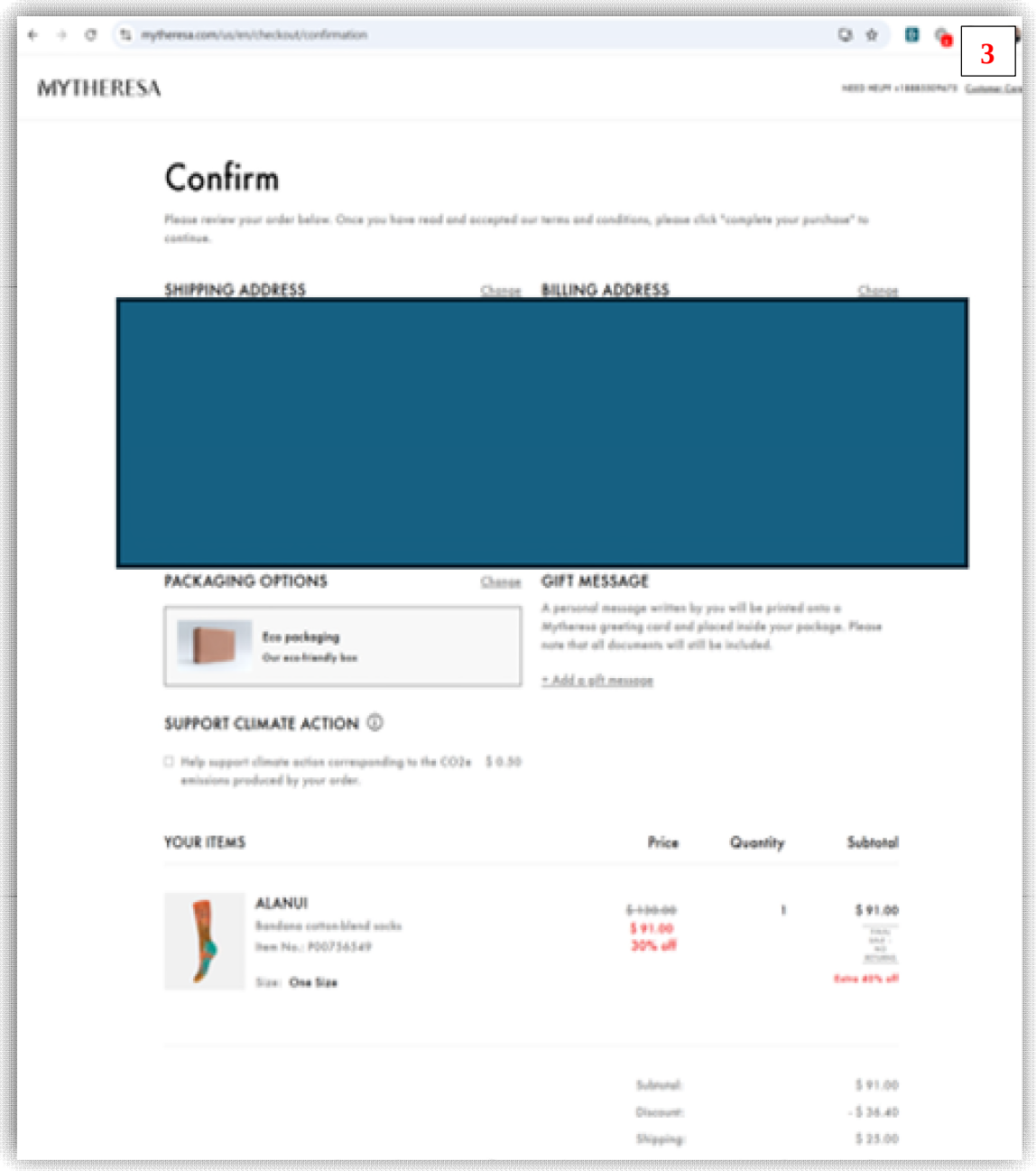
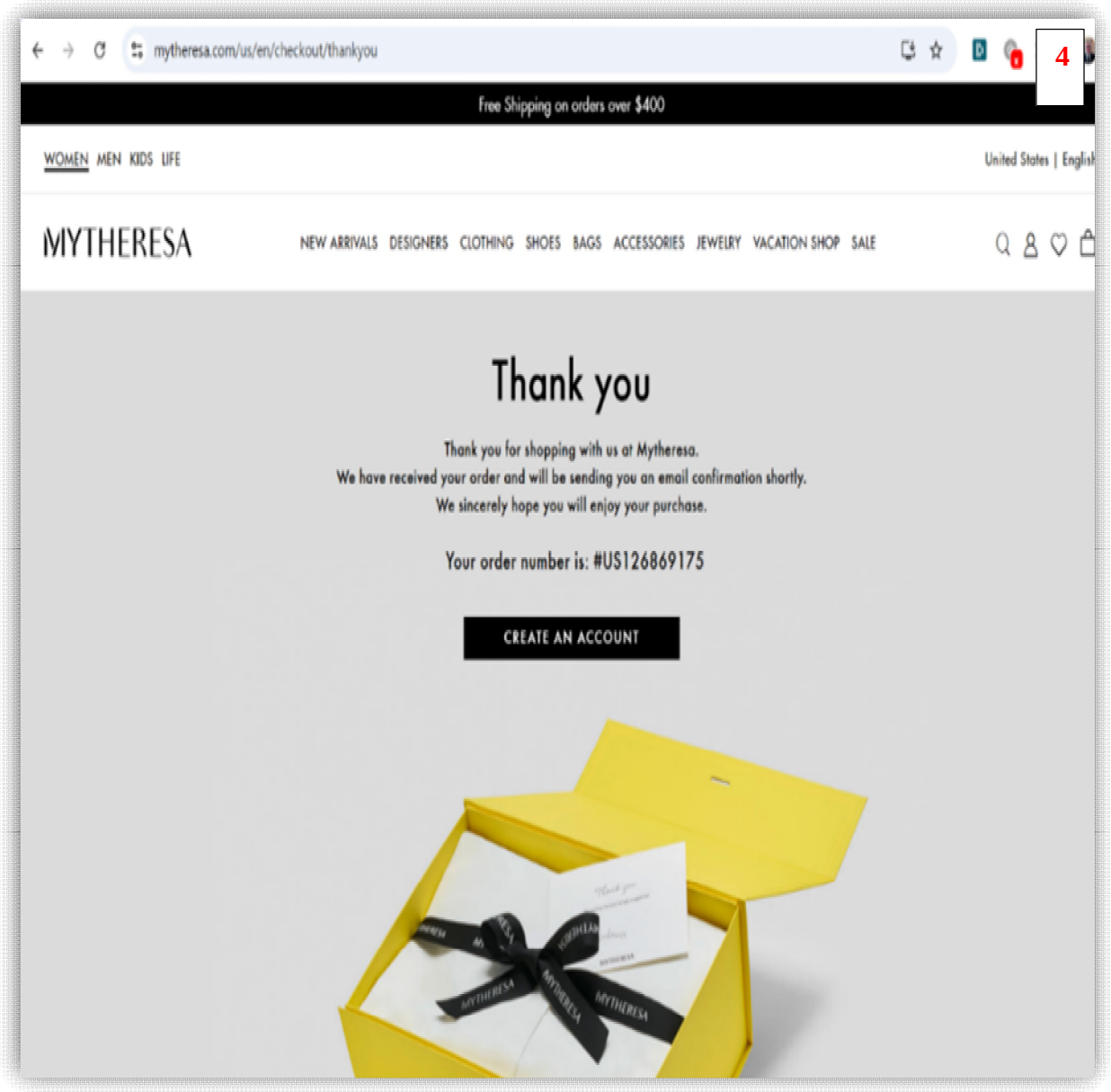



Image 2: In the cookies stored on the buyer's browser from the moment the user lands on the Mytheresa webpage after clicking on the Madison Avenue Spy affiliate link, and that remains stored on the browser all the way through checkout and post-checkout, a cookie called "click_session" denotes that the "referrer" for the sale is "maidsonavenuespy.com"

61. As the buyer moves through the checkout process on Mytheresa, the cookie naming Madison Avenue Spy as the referrer persists. Mytheresa would know to award Madison Avenue Spy commission for any sale that was consummated as a result of a buyer following her affiliate link and completing a purchase on Mytheresa's webpage because this cookie stored in the buyer's browser credits Madison Avenue Spy with the purchase—from the moment that the buyer lands

on the Mytheresa webpage after clicking on the Madison Avenue Spy affiliate link through the completion of the buyer's purchase. As explained below, the cookie stores this information so long as the buyer never engages with the Capital One Shopping browser extension during the checkout process.






Images 3 and 4: The buyer moves through the checkout process without engaging with the Capital One Shopping browser extension and completes a purchase for a pair of bandana cotton-blend socks with Product SKU P00756549.

62. In this scenario, the creator gets credit for the referral and is entitled to receive a commission from the online merchant. When Madison Avenue Spy reviews her commissions, she sees earnings totaling $5.67 for the conversion of the buyer from her affiliate link to a completed purchase of the Mytheresa bandana cotton-blend socks product with Product SKU D_P00756549 on March 20, 2025, at or around 12:30pm EST.

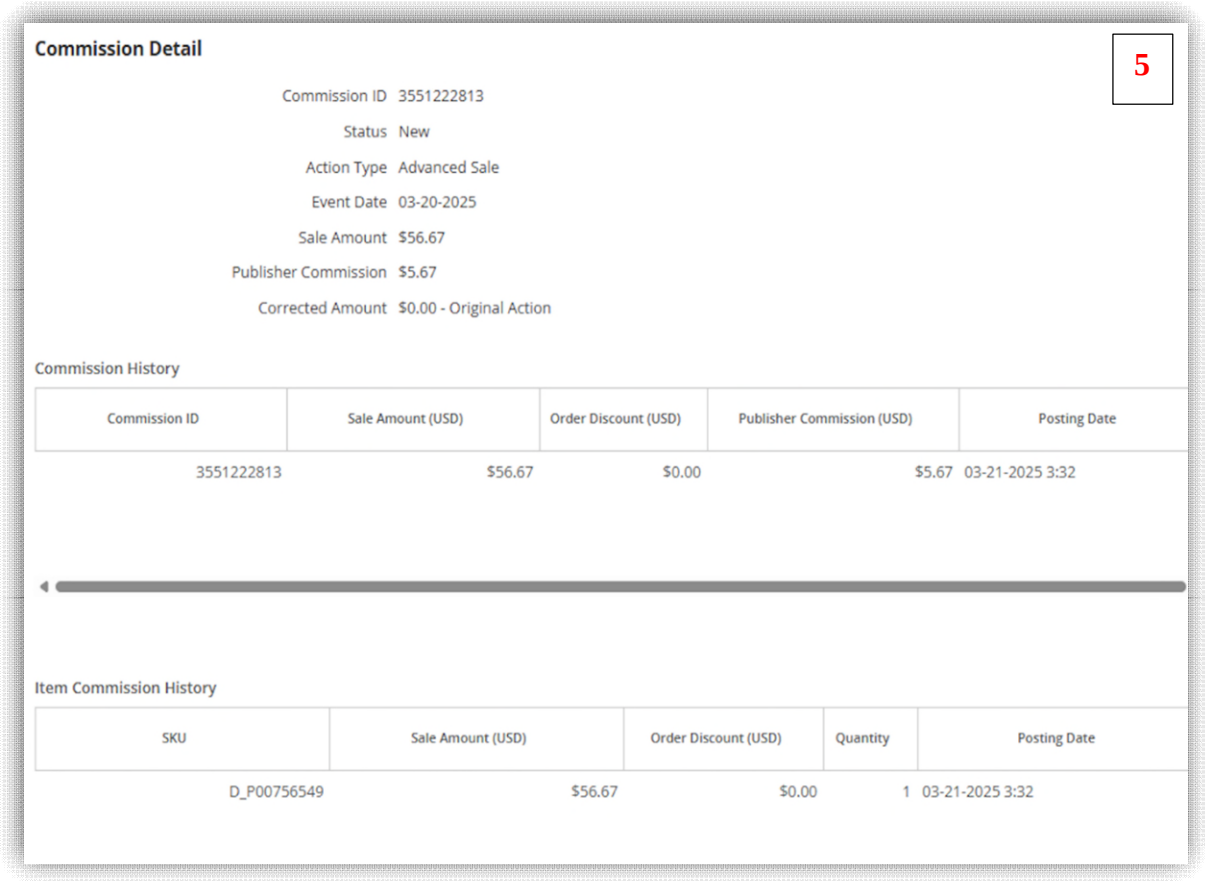



Image 5: A screenshot of Madison Avenue Spy's CJ Affiliate dashboard showing her commission for a buyer's purchase of bandana cotton-blend socks on Mytheresa.

63. However, as explained further in the subsequent section, in certain circumstances, Madison Avenue Spy does not receive commissions from merchants for completed sales after referring consumers to a merchant's webpage via her affiliate links. Despite being entitled to these commissions, Madison Avenue Spy is deprived of them as a result of Capital One's illegal conduct.

**6. Capital One's Exploitation of Last-Click Attribution**

64. Capital One uses the Capital One Shopping browser extension to manipulate consumers' website traffic and network traffic transmissions, namely by artificially manufacturing a click on behalf of the consumer. This artificially manufactured click makes it *appear* to the browser and merchant that a consumer has navigated from a *different location* on the internet – namely, a Capital One affiliate link—to the merchant's webpage to make a purchase from that merchant. This occurs despite the fact that the consumer was already on the merchant's site.

65. Capital One's artificially manufactured click enables the extension to replace the affiliate tracking codes that are stored on consumers' devices (usually as cookies) and transmitted during the checkout process with tracking codes that credit Capital One with the referral, the purchase, and ultimately the commission generated by the sale.

66. Put differently, the Capital One Shopping browser extension is designed to simulate a legitimate "last click" by making it appear as though the consumer clicked on a Capital One link to navigate to the merchant's page. In all reality, however, no such click occurred.

67. The Capital One Shopping browser extension does this by injecting a hidden tab, which redirects a consumer's browser to a purpose-built URL, to overwrite the previous affiliate tracking code with Capital One's own. When the extension injects this hidden tab after a consumer visits a merchant's website from an affiliate link, Capital One knows that it is stealing the commission from the creator who is entitled to the commission—the creator whose link was the consumer's "last click" that caused the consumer to navigate to the merchant's site.

68. This allows Capital One to surreptitiously take credit for sales it did not refer to the merchant—without any Capital-One-driven "click" from the consumer to navigate to the merchant's webpage. In fact, the consumer does not even engage with the Capital One Shopping

browser extension until the consumer is already on the checkout page of the merchant's website.

69. It is at this point that the Capital One Shopping browser extension displaces the affiliate tracking codes that identify creators as the source of the referral, substitutes Capital One's own tracking codes, and improperly holds Capital One out as the "last click"—that is, the referrer of the specific products or services.

70. Capital One does this even when it knows or should know that the sale in question originated from a creator's affiliate link, not a Capital One Shopping referral link.

71. Capital One comprehensively monitors browsing history URLs that contain both: (1) other affiliate tracking codes (including from creators like Plaintiffs) and (2) its own overwritten affiliate codes. In other words, Capital One has information about both existing affiliate tracking codes and the Capital One Shopping browser extension's displacement of those codes.

72. More specifically, and as depicted in the images below, the Capital One Shopping browser extension is designed to continuously upload detailed logs to its server at track.capitaloneshopping.com contemporaneously with a consumer's browsing.

73. These logs include, among other detailed information, the full-string URL of each web page visited by a consumer.[27]

74. From these full-string URLs, Capital One knows (or should reasonably know) precisely when a consumer has navigated to a specific merchant's website using a specific affiliate's referral link.

[27] For instance, for Plaintiff ToastyBros, that URL would be: https://www.newegg.com/abs-sa14400f4060ti-stratos-aqua/p/N82E16883360464?utm_campaign=afc-howl-toastybros-qp1sfsvpxsqhf&nrtv_cid=qp1sfsvpxsqhf&utm_medium=affiliate&utm_source=howl-toastybros.

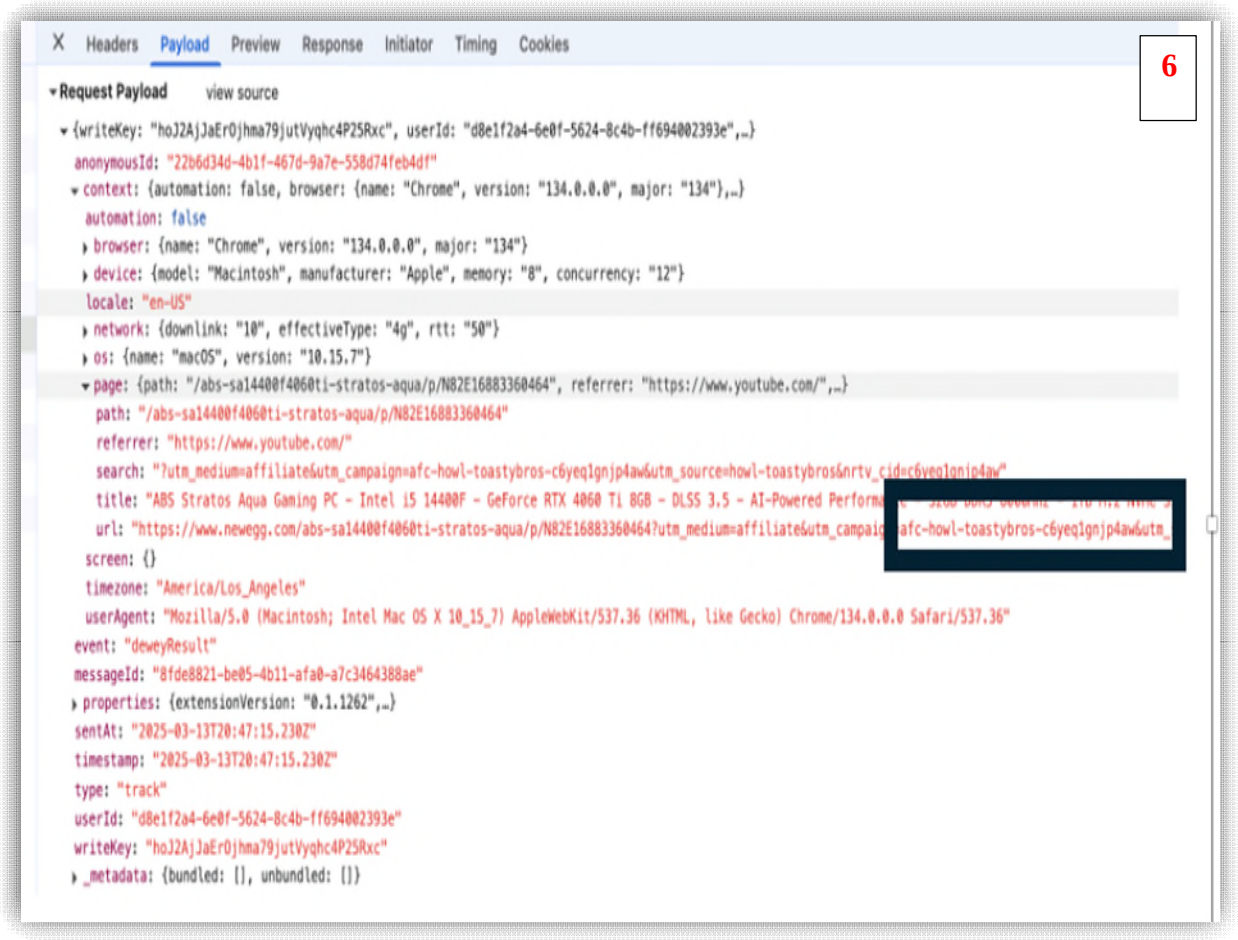



Image 6: This shows a packet of information transmitted to and received by the Capital One Shopping browser extension after a buyer[28] visits the Newegg online webpage after having clicked on an affiliate URL shared by ToastyBros. This information packet identifies ToastyBros as the affiliate in the merchant's URL.

[28] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

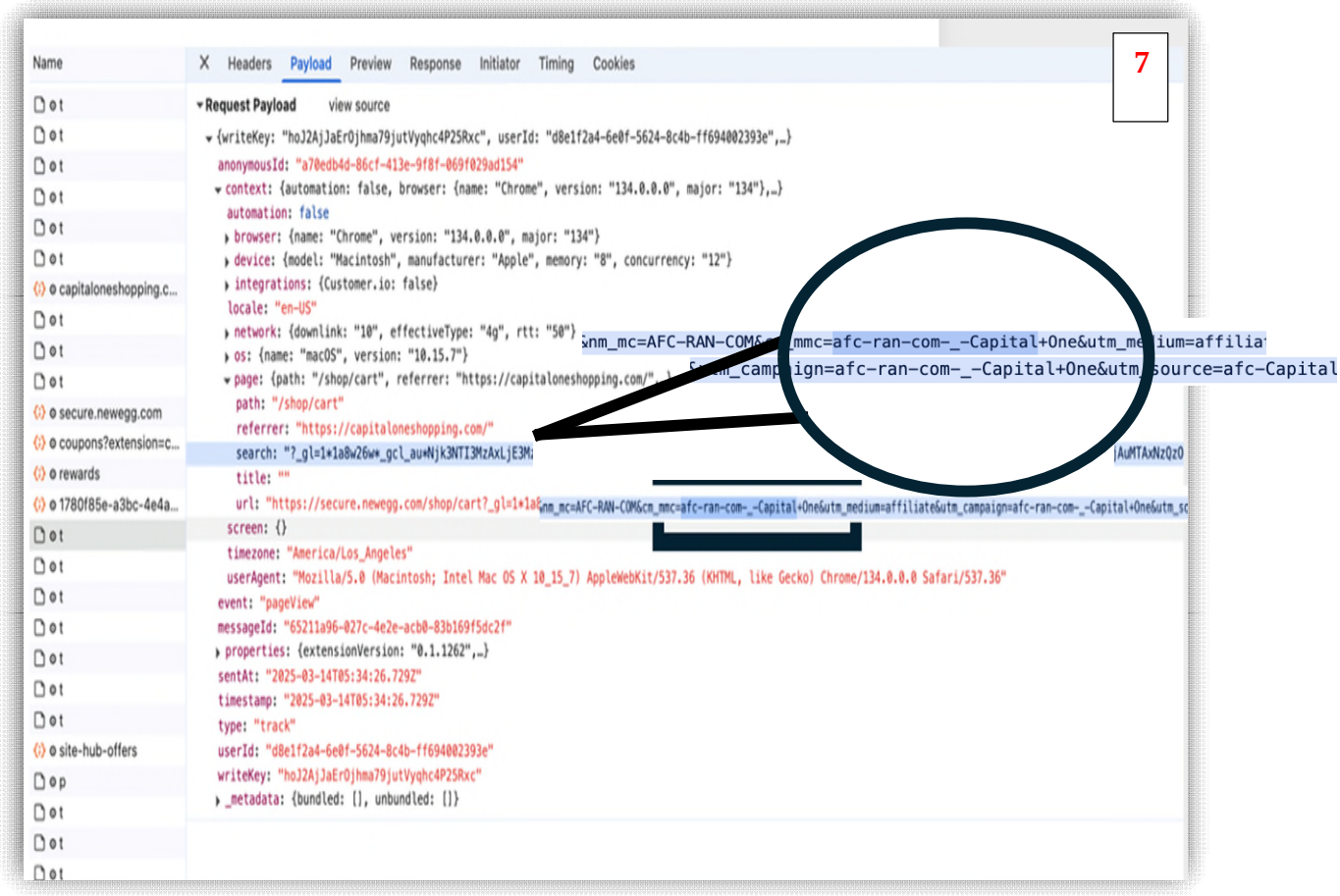



Image 7: This shows a packet of information transmitted to and received by the Capital One Shopping browser extension after a buyer uses the Capital One Shopping browser extension to "try codes" at check out. This information packet identifies Capital One as the affiliate in the merchant's URL.

75. In other words, Capital One's servers receive and store information about the identity of the referring affiliate in every instance in which the browser extension is engaged and in every instance in which the extension displaces that information with its own affiliate tracking code.

76. The Capital One Shopping browser extension is purposely designed to exploit the last-click attribution process and the operation of affiliate tracking codes, and it achieves this by surreptitiously forcing refreshes of a merchant's checkout page, which the consumer is already on, by enticing a consumer to use the Capital One Shopping browser extension to test out coupon

codes or activate rewards offered by the extension. The Capital One browser extension forced refresh results in the simulation of a click from a different site to the merchant's site, and thus allows Capital One to inject affiliate tracking codes associated with Capital One, which displace any existing affiliate tracking codes. This ultimately results in Capital One being credited as having referred the consumer to the merchant as the "last click." In all reality, however, the consumer was *already on* the merchant's site.

77. Capital One created its extension to require the consumer to click on their pop-up because it is this engagement which technologically enables Capital One to masquerade as though a Capital One referral link was the "last click" the consumer made in the course of navigating to the merchant's page. Stated differently, Capital One has designed its browser extension in a manner that requires consumers to actively engage with the browser extension—i.e., click buttons—to search for a discount or rewards. These clicks are important to Capital One because they facilitate Capital One's technical capability to simulate a legitimate "last click"—that is, a click that the consumer used to navigate to the merchant's site.

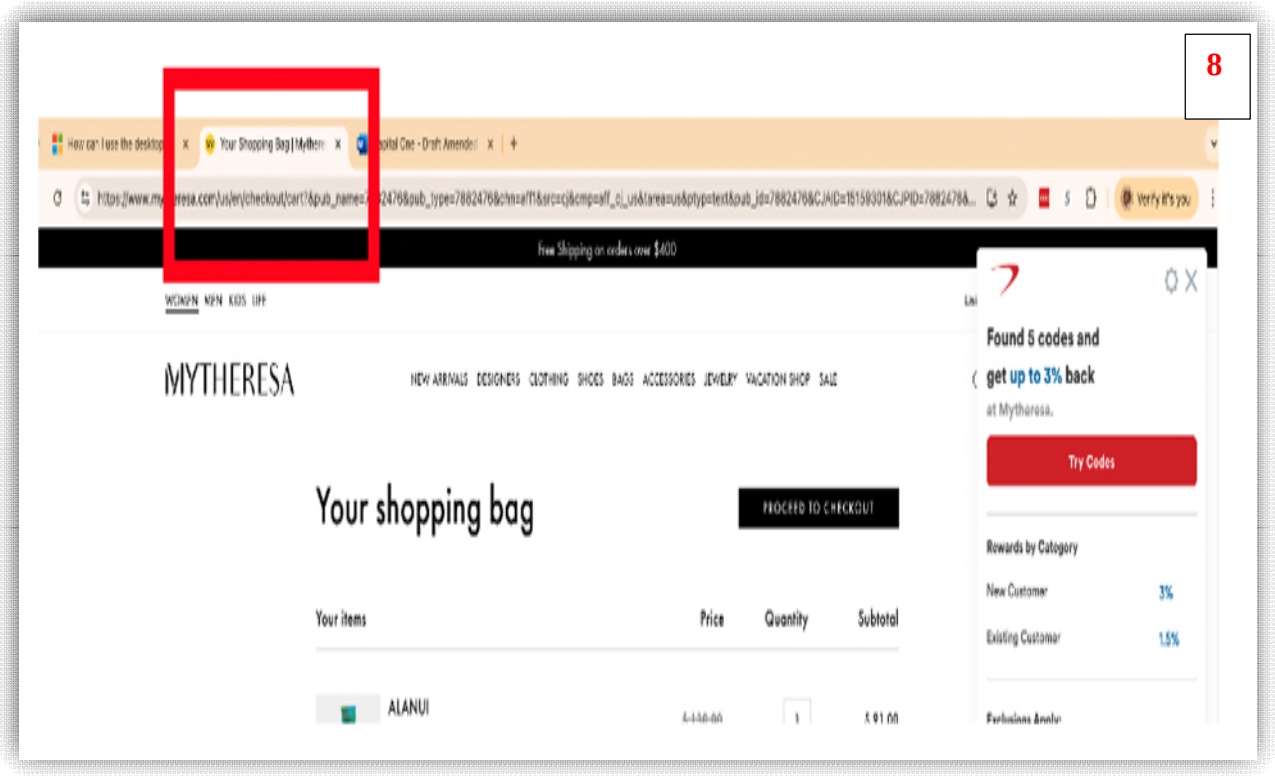
78. Capital One achieves this simulated "last click" because the extension is programmed to elicit clicks from the consumer. These consumer clicks, in turn, trigger the extension to open an ephemeral, hidden tab.[29] Capital One injects a "redirect" URL into this new tab, which forces a refresh onto the merchant page, mimicking a new click by the consumer from a Capital One affiliate link back onto the merchant checkout page. This sleight of hand occurs despite the fact that the consumer was already on the merchant's page and got there by way of a creator's referral link.

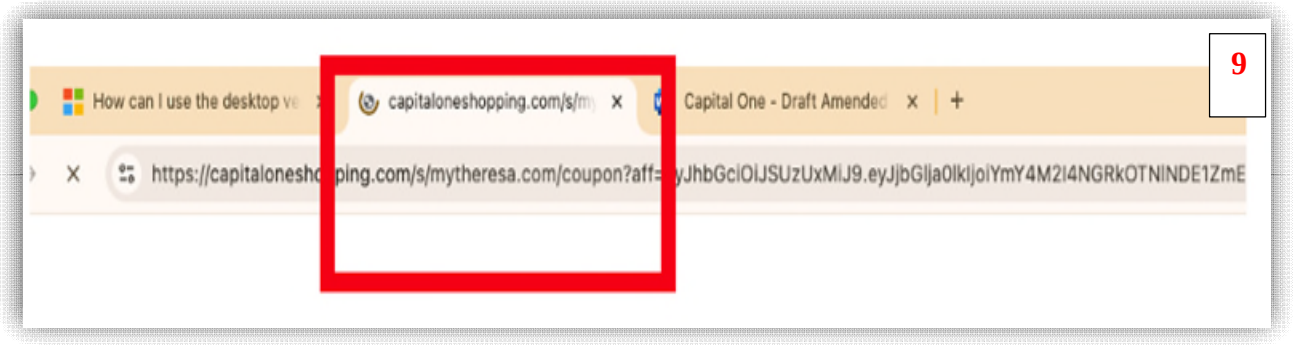
[29] This simulated click is generated either by the Capital One Shopping browser extension forcing a refresh of the merchant's product page that the consumer is already on or by discreetly opening a small new tab on the consumer's web browser.

79. Capital One's forced refresh of the merchant's page causes the affiliate tracking codes—usually cookies—stored in the consumer's browser to falsely indicate to the online merchant that the consumer clicked on Capital One's—rather than the creator's—hyperlink to land on the merchant's page.

80. By performing this sleight of hand, Capital One gets credit for referring a consumer to the merchant's page, despite the fact that the consumer arrived om the merchant's website based on the creator's recommendation and using the creator's affiliate link, *not* by clicking on Capital One's browser extension.

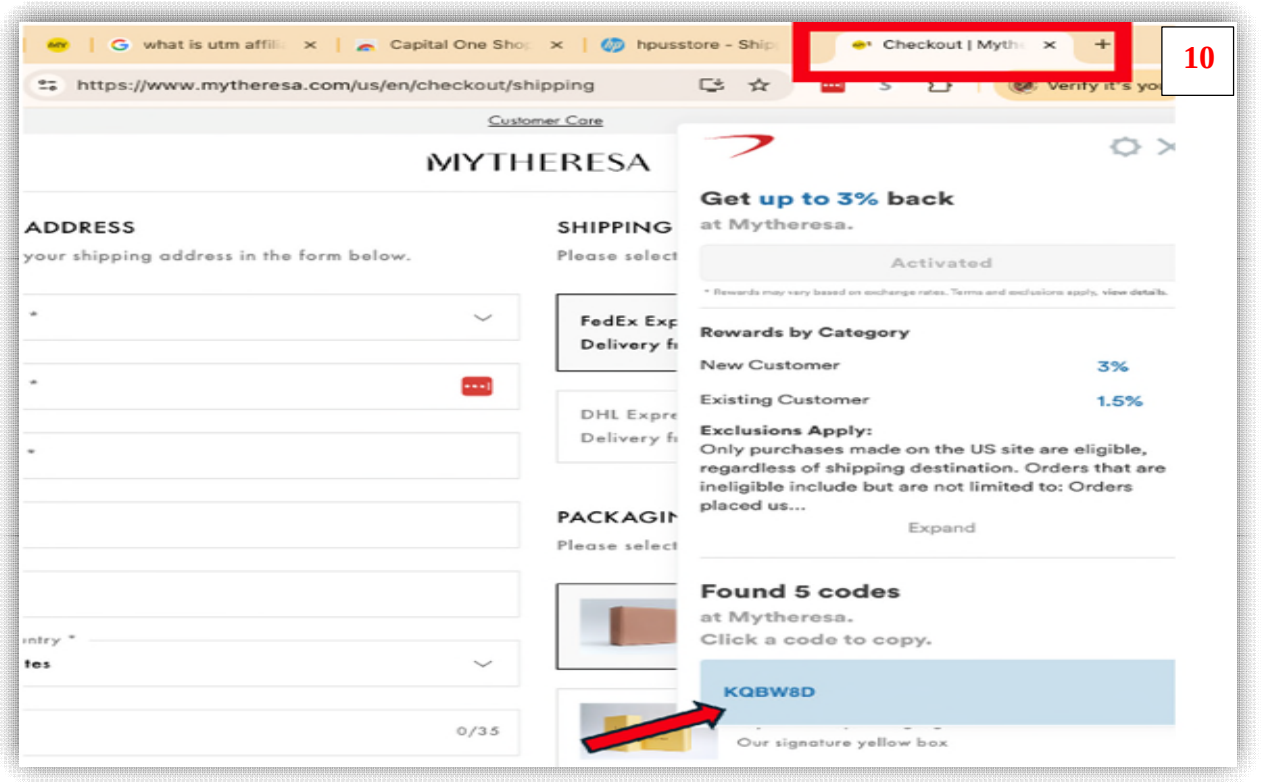
81. With this bait-and-switch complete, Capital One automatically closes the small tab with the consumer none the wiser.






Images 8 and 9: In **Scenario A (above)**, after electing to "Try Codes" in the Capital One Shopping browser extension, the buyer's shopping bag automatically refreshes, temporarily displaying a capitaloneshopping.com URL that persists for long enough to simulate a click by the buyer on a Capital One affiliate link.[30] This automatic refresh displaces the creator's affiliate tracking code and inserts Capital One's own tracking code as the referrer of the sale.

Image 10: Alternatively, in **Scenario B (Below),** after the buyer attempts to apply a code that the Capital One Shopping browser extension located to the buyer's purchase at checkout, the extension opens a second mini-tab that automatically refreshes the main product page (top left-hand corner above the refresh button). As in Scenario A, Capital One's automatic refresh injects code into the URL bar that simulates a click by the buyer on a Capital One affiliate link, displacing the creator's affiliate tracking code and inserting Capital One's own tracking code as the referrer of the sale.




[30] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

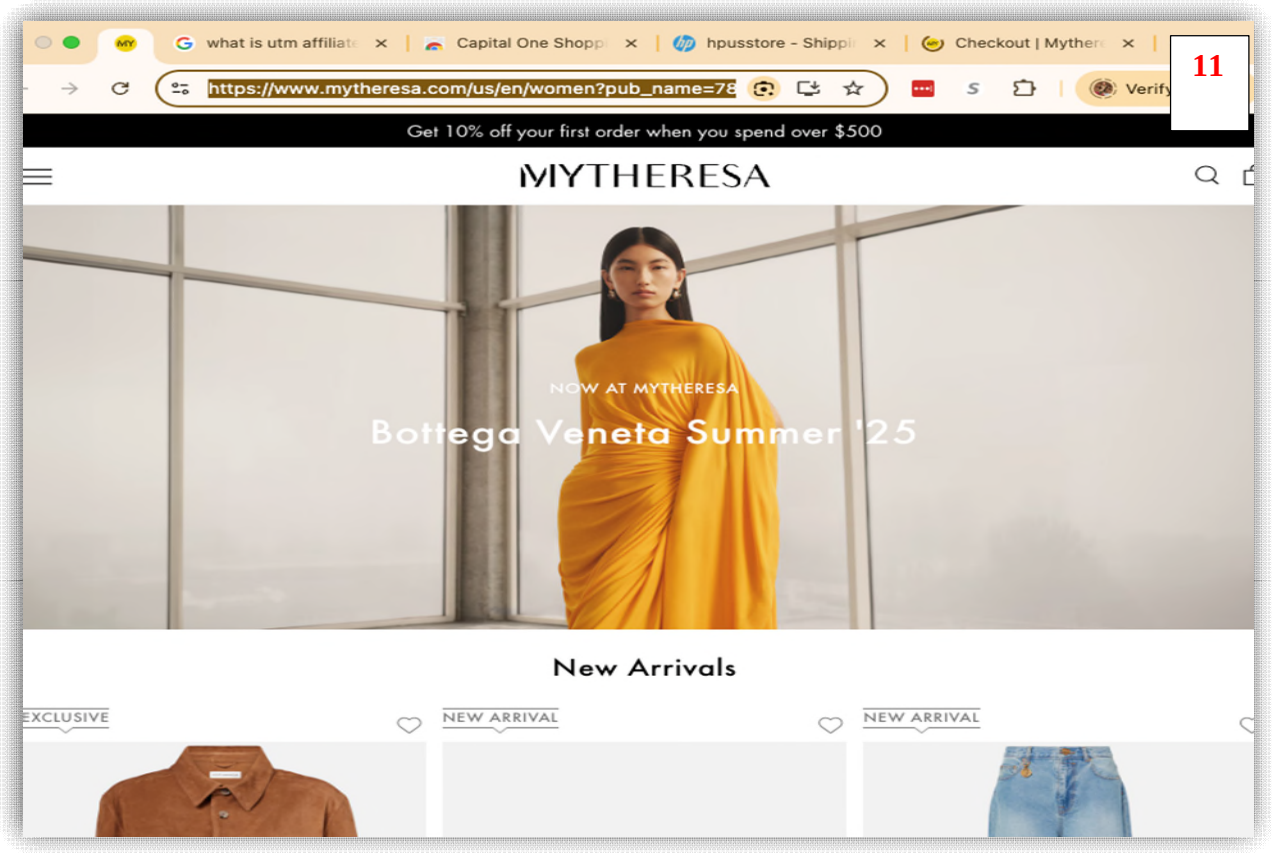



Image 11: The contents of the mini-tab artificially opened by the Capital One Shopping browser extension shows the merchant's webpage is opened a second time is a replication of the merchant page that the buyer already has open. The mini-tab automatically closes after it injects affiliate tracking code into the buyer's browser that tricks the merchant into believing that CapitalOne—and not the creator—was the referring source of the sale.

82. The result of Capital One's programming scheme is that Capital One steals the last-click attribution for the sale of the online merchant's product or service and thus gets paid a commission by the online merchant on the sale despite the fact that Capital One played no role in referring the consumer to the online merchant's website.

83. Meanwhile, the creator is left without a commission despite having put in the time and effort to create the promotional content for the online merchant's product or service that caused a consumer thereof to click on the creator's affiliate link for and ultimately purchase the merchant's promoted product or service.

84. An analysis of Madison Avenue Spy's affiliate activity demonstrates this stolen conversion.

85. When a buyer[31] *with* the Capital One Shopping browser extension installed navigates to the online merchant Mytheresa's webpage by clicking on an affiliate link shared by Plaintiff Madison Avenue Spy and lands on the Mytheresa webpage, if the buyer completes a purchase on Mytheresa without having navigated away from the Mytheresa webpage or clicking on any intervening affiliate marketing URLs that also direct the buyer to Mytheresa, Madison Avenue Spy is entitled to receive a commission for any purchase made by the buyer on Mytheresa's webpage.

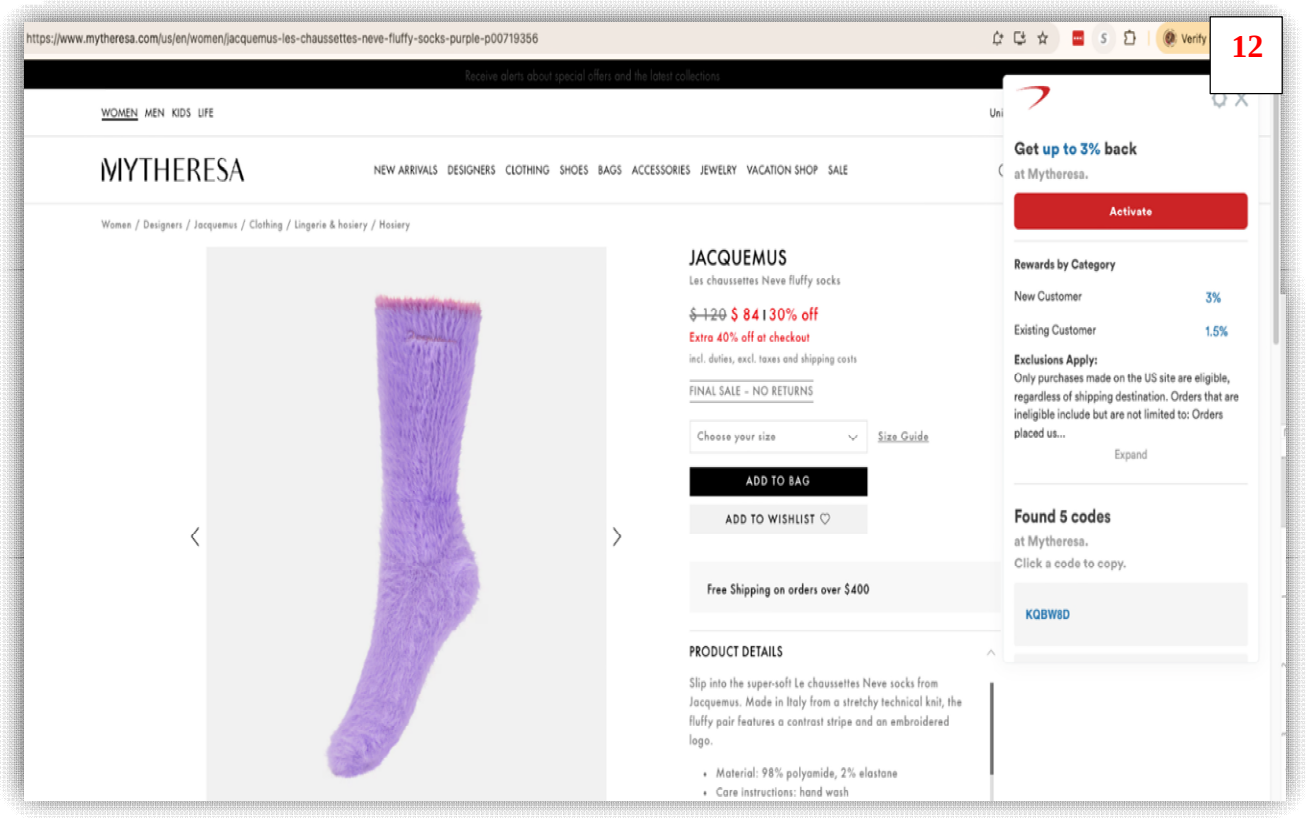



Image 12: A buyer navigates to a Mytheresa product page by clicking on an affiliate link shared by Plaintiff Madison Avenue Spy on her fashion blog which links to Mytheresa.

[31] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

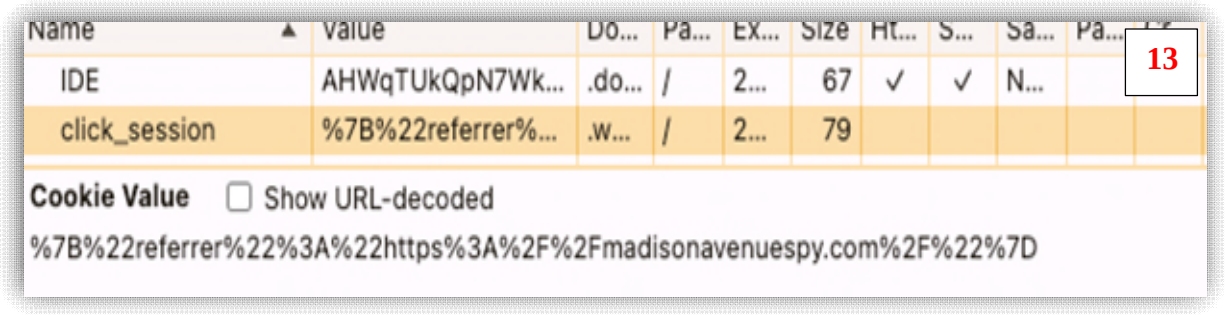



Image 13: Before engaging with the Capital One Shopping browser extension, the cookie value for "click_session" stored in the buyer's browser denotes "madisonavenuespy.com" as the referrer of the sale.

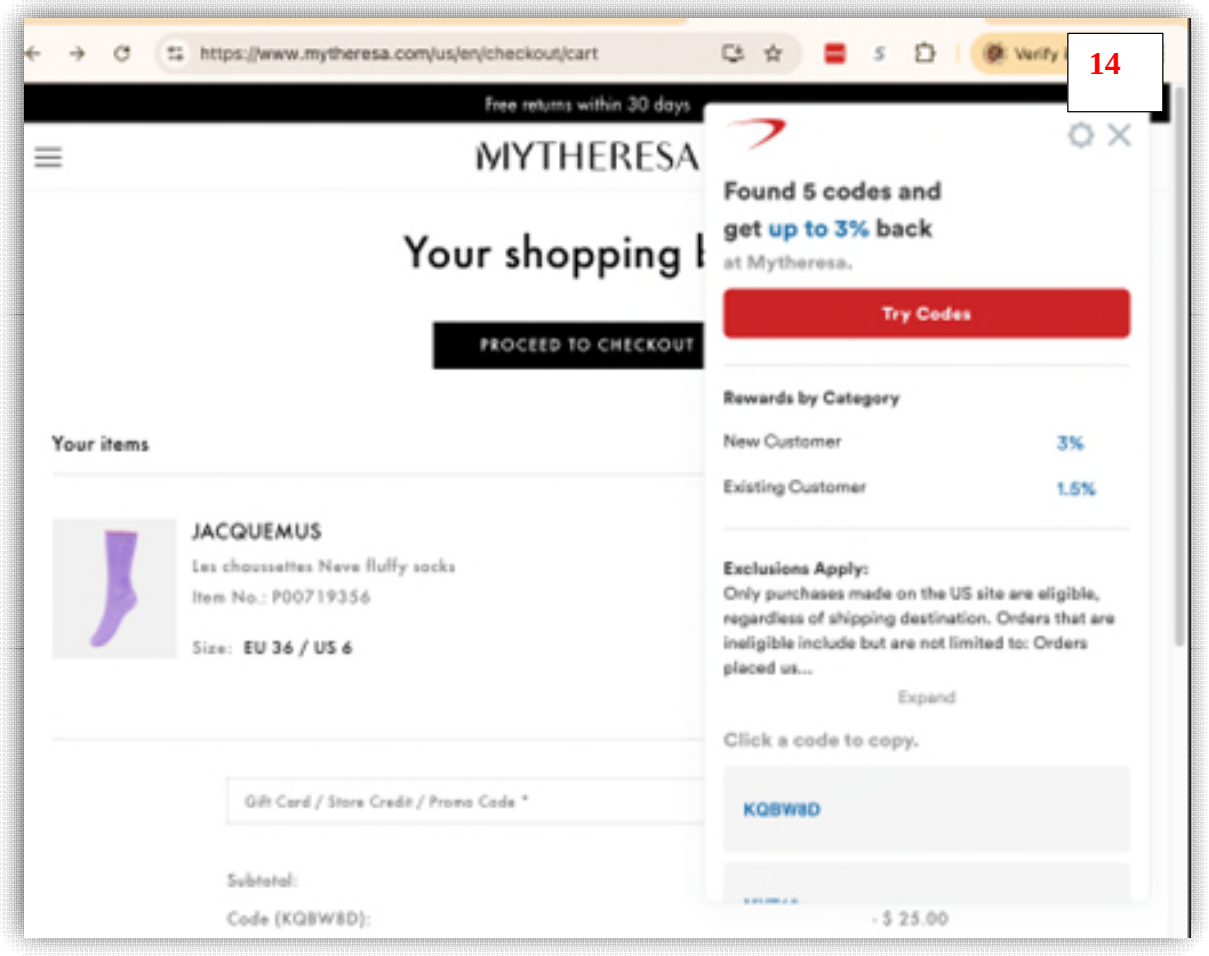
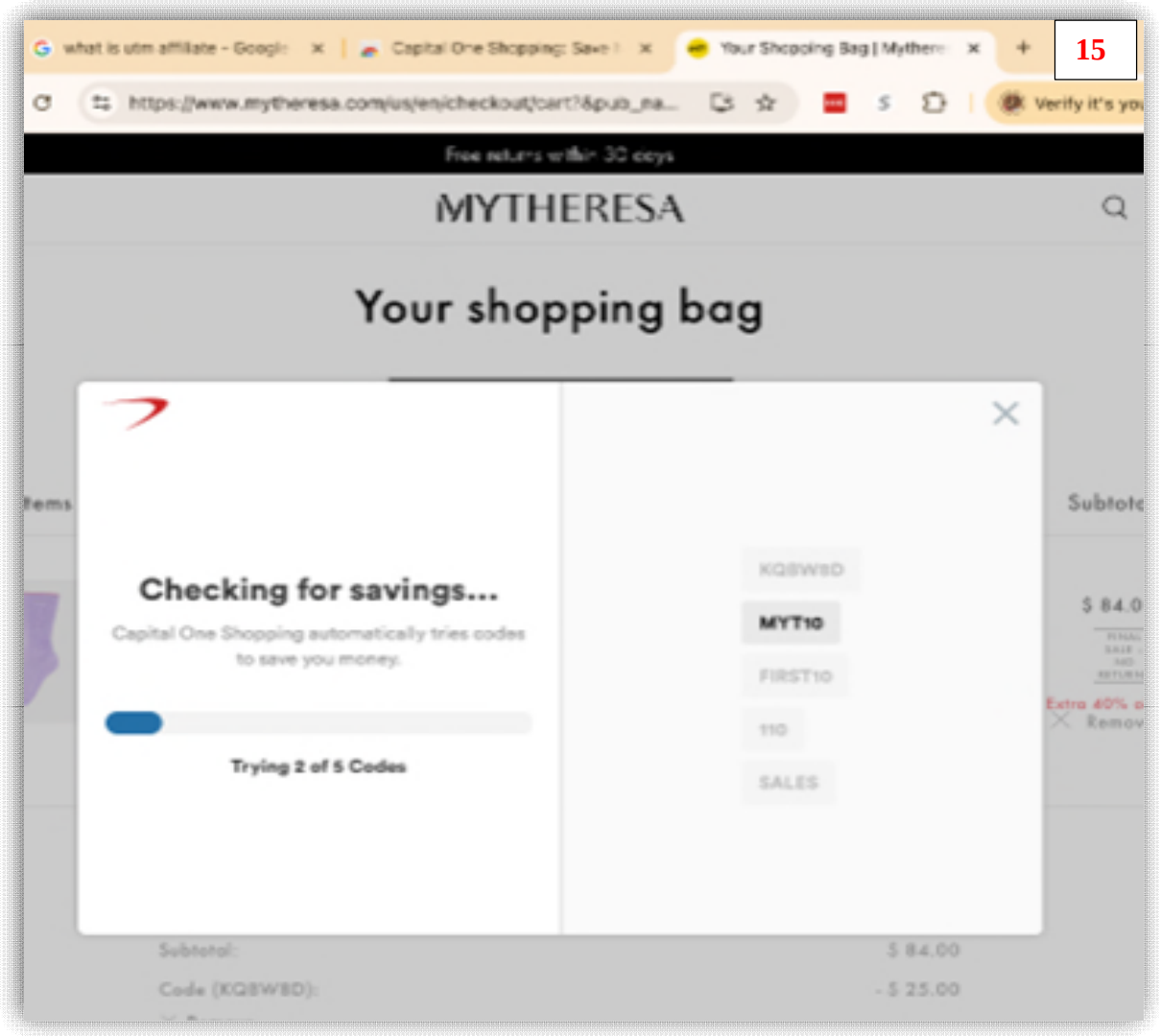



Image [14]: On the Mytheresa checkout page, the buyer, about to complete a purchase after following Madison Avenue Spy's affiliate link, is prompted by Capital One to "Try Codes" through its browser extension. The buyer accepts the offer.

Images 15 and 16 (below): The buyer allows the Capital One Shopping browser extension to try various coupon codes. Before initiating the pop-up reading “Checking for savings...” on the Mytheresa checkout page that the buyer was already on, the Capital One Shopping browser extension surreptitiously forces a refresh of the checkout page that simulates a referral click on an affiliate link, thereby giving Capital One credit for being the referrer of the sale.



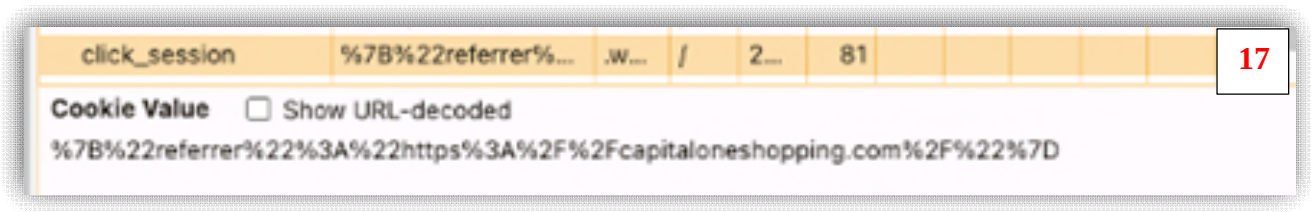
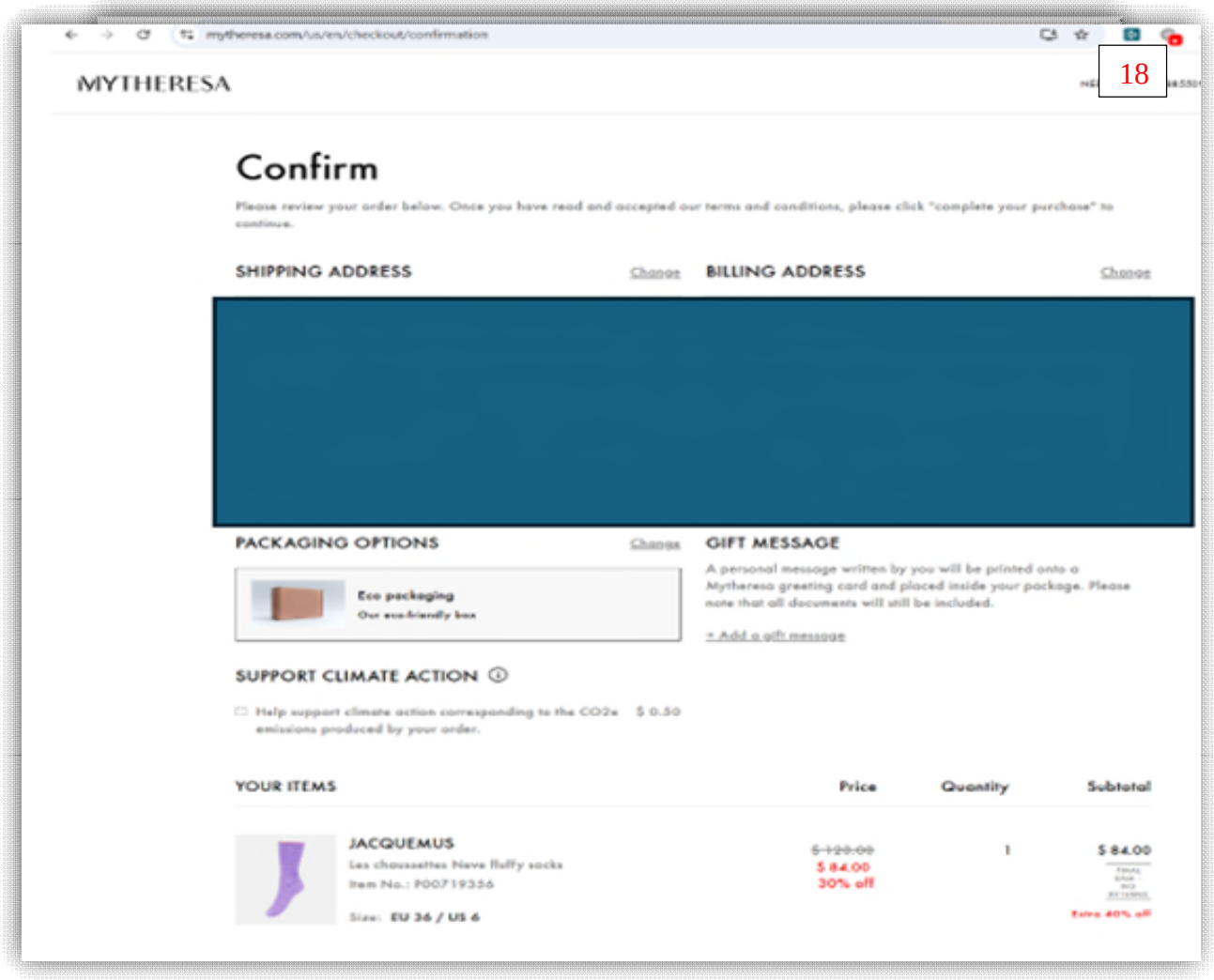
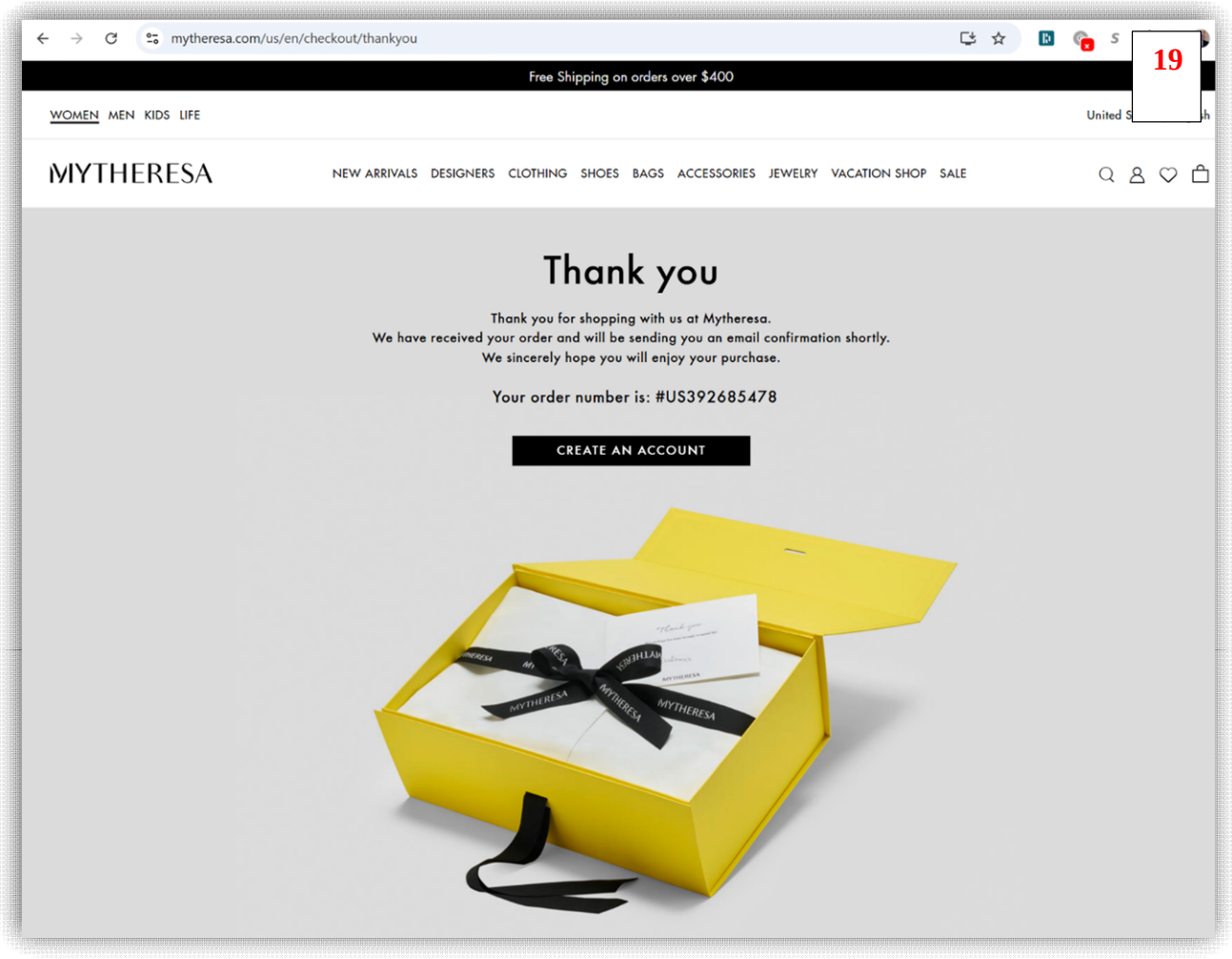




Image 17: After the extension surreptitiously force-refreshes the Mytheresa checkout page, the buyer's browser displaces "madisonavenuespy.com" as the value of the "click_session" cookie stored in the buyer's browser. After that surreptitious refresh which simulates a referral click, the value of the "click_session" indicates that "captialoneshopping.com" is the referrer of the sale.

Images 18 and 19 (below): The buyer moves through checkout to complete the purchase after activating Shopping Rewards through the Capital One Shopping browser extension.






86. However, when Plaintiff Madison Avenue Spy reviews her commissions for the purchase made by the buyer on March 20, 2025, at or around 12:54pm EST after the buyer engaged with the Capital One Shopping browser extension, she sees no commission for the conversion of the buyer from her affiliate link to a completed purchase of the Mytheresa product, despite the fact that the buyer never knowingly clicked on an intervening affiliate link, never navigated away from the Mytheresa page at all, and only engaged with the Capital One Shopping browser extension after already reaching the product-purchase page on Mytheresa's website. In other words, even though Plaintiff Madison Avenue Spy was entitled to receive a commission on this transaction,

she did not receive it.

87. The same outcome is observed for Plaintiff Just Josh after a buyer[32] uses Just Josh's affiliate web links to visit Best Buy's merchant webpage and complete a purchase under two conditions: with and without engaging with the Capital One Shopping browser extension.

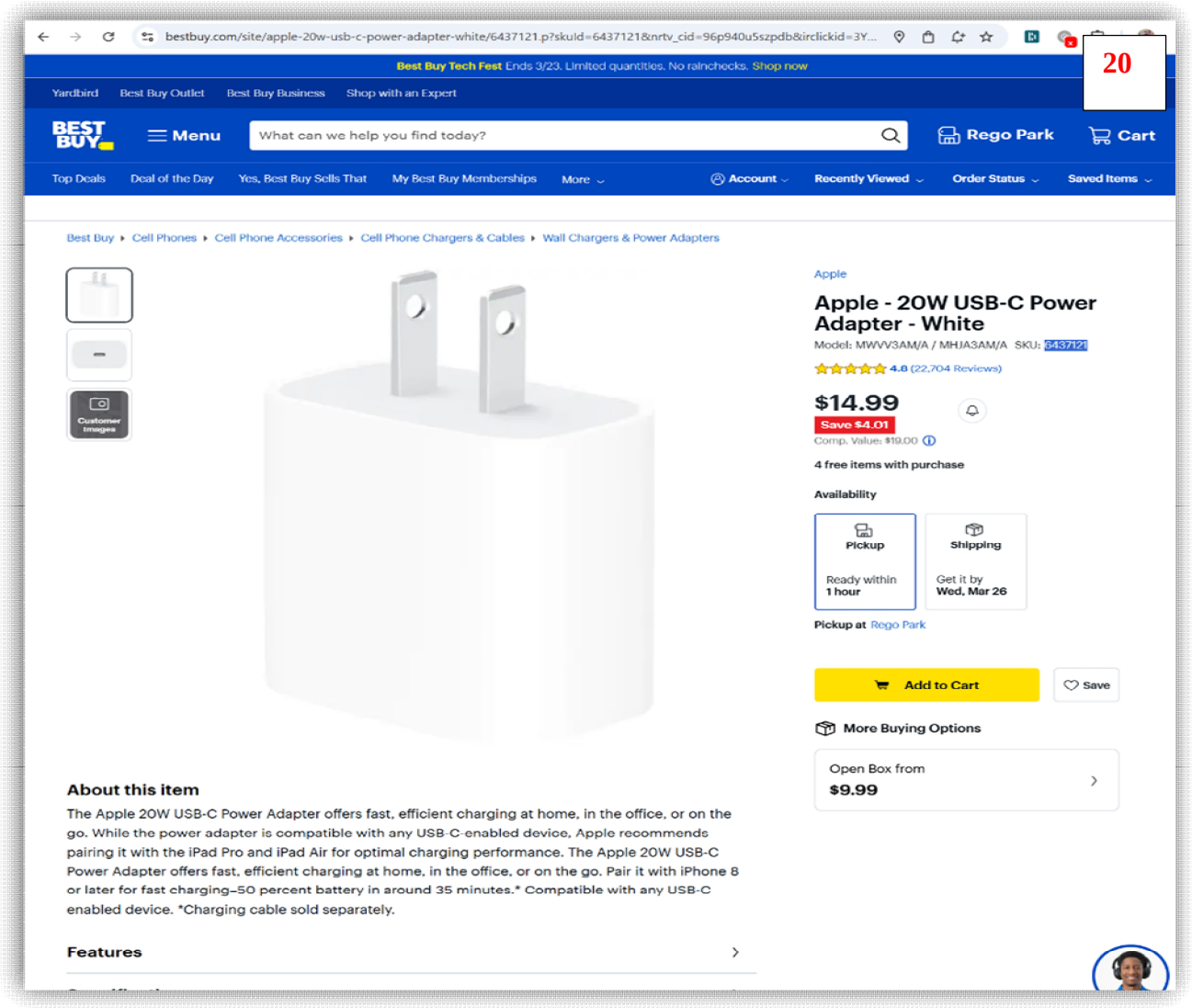
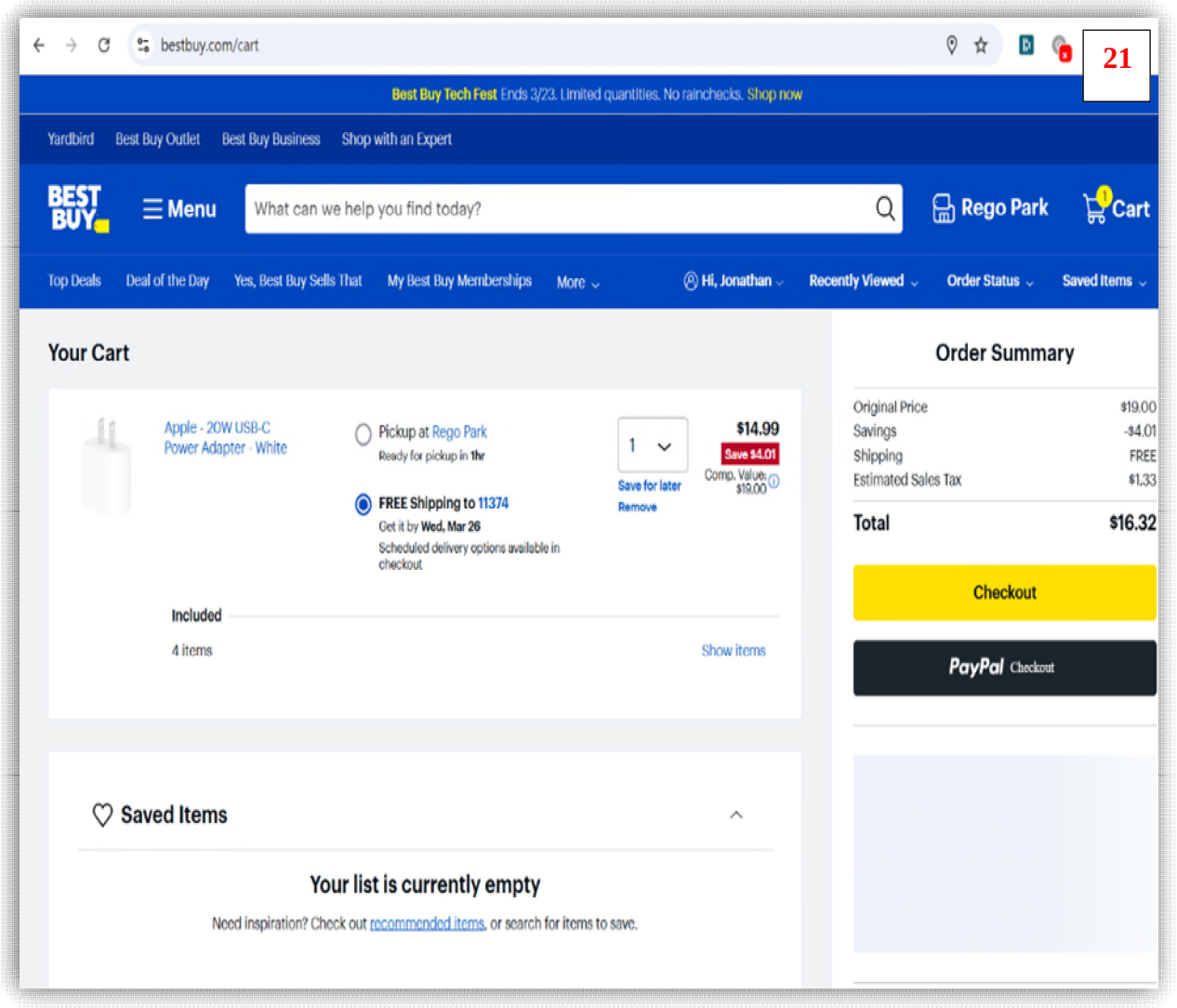


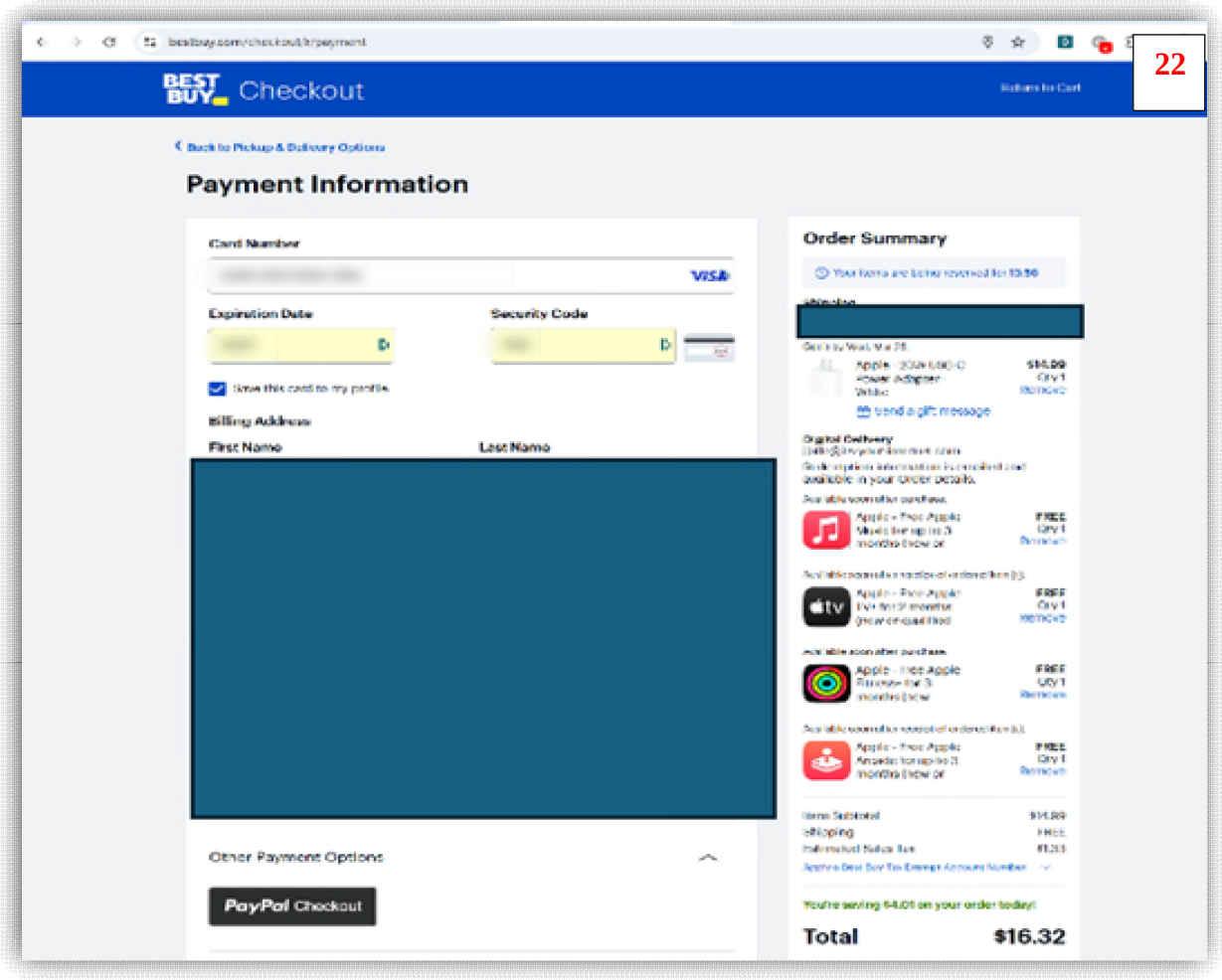

Image 20: The buyer follows Just Josh's affiliate link to the Best Buy merchant page and moves through the steps to checkout and complete a purchase for an Apple Power Adapter.

[32] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

88. In scenario one—where a buyer *does not* engage with the Capital One Shopping browser extension—when the buyer clicks on Just Josh's affiliate link for Best Buy and the buyer completes a purchase on Best Buy, Just Josh's affiliate tracking code persists in the buyer's browser from the moment the consumer lands on the Best Buy webpage until after the buyer completes the purchase. As a result, Just Josh is entitled to a commission earned for referring the sale to Best Buy.

Images 21, 22, and 23: The buyer completes an order on Best Buy after following Just Josh's affiliate link to Best Buy's webpage.




22
BEST BUY Checkout
Payment Information
Card Number
Expiration Date
Security Code
Billing Address
First Name
Last Name
Other Payment Options
PayPal Checkout
Order Summary
Total
$16.32

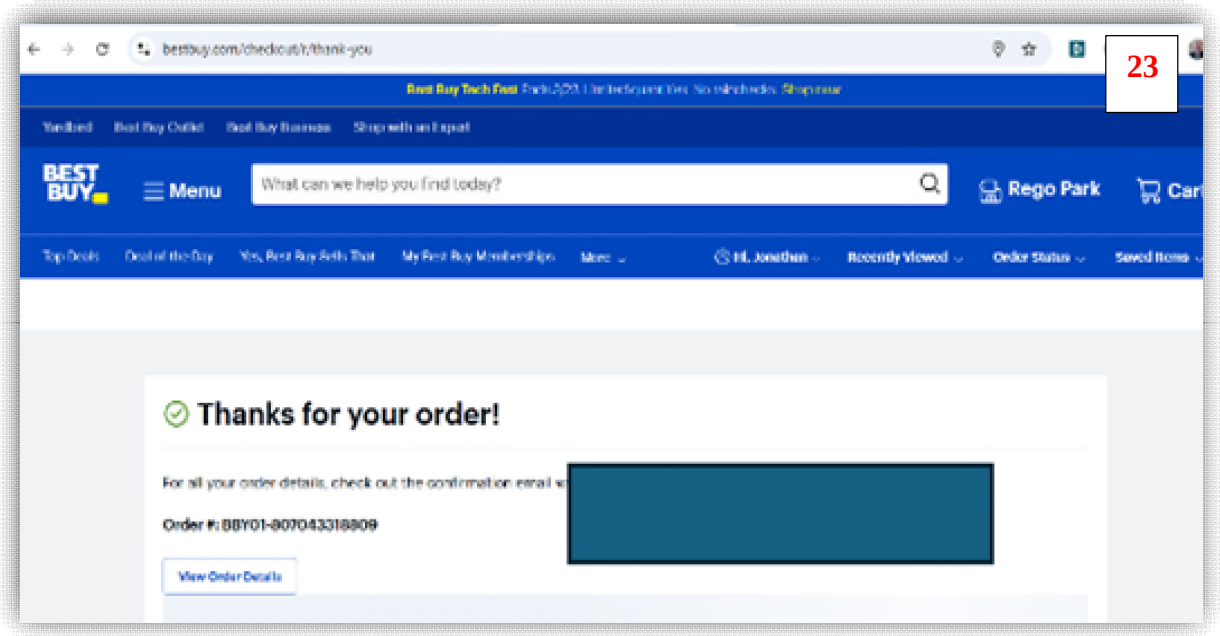
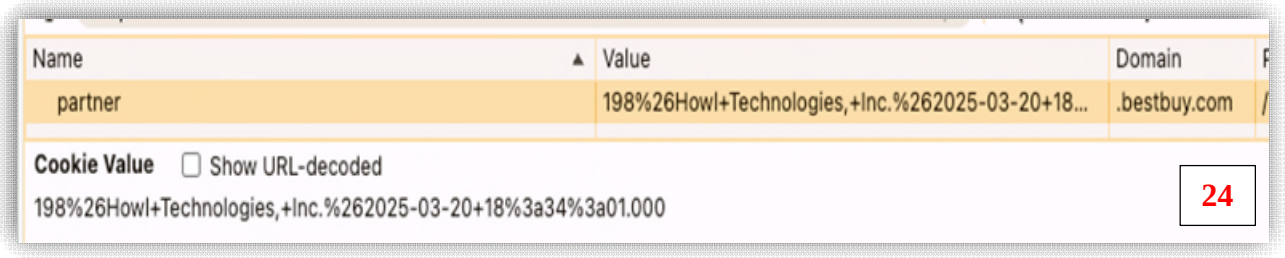

23
BEST BUY
Menu
What can we help you find today?
Rego Park
Thanks for your order!
Order #: BBY01-807043318809
View Order Details

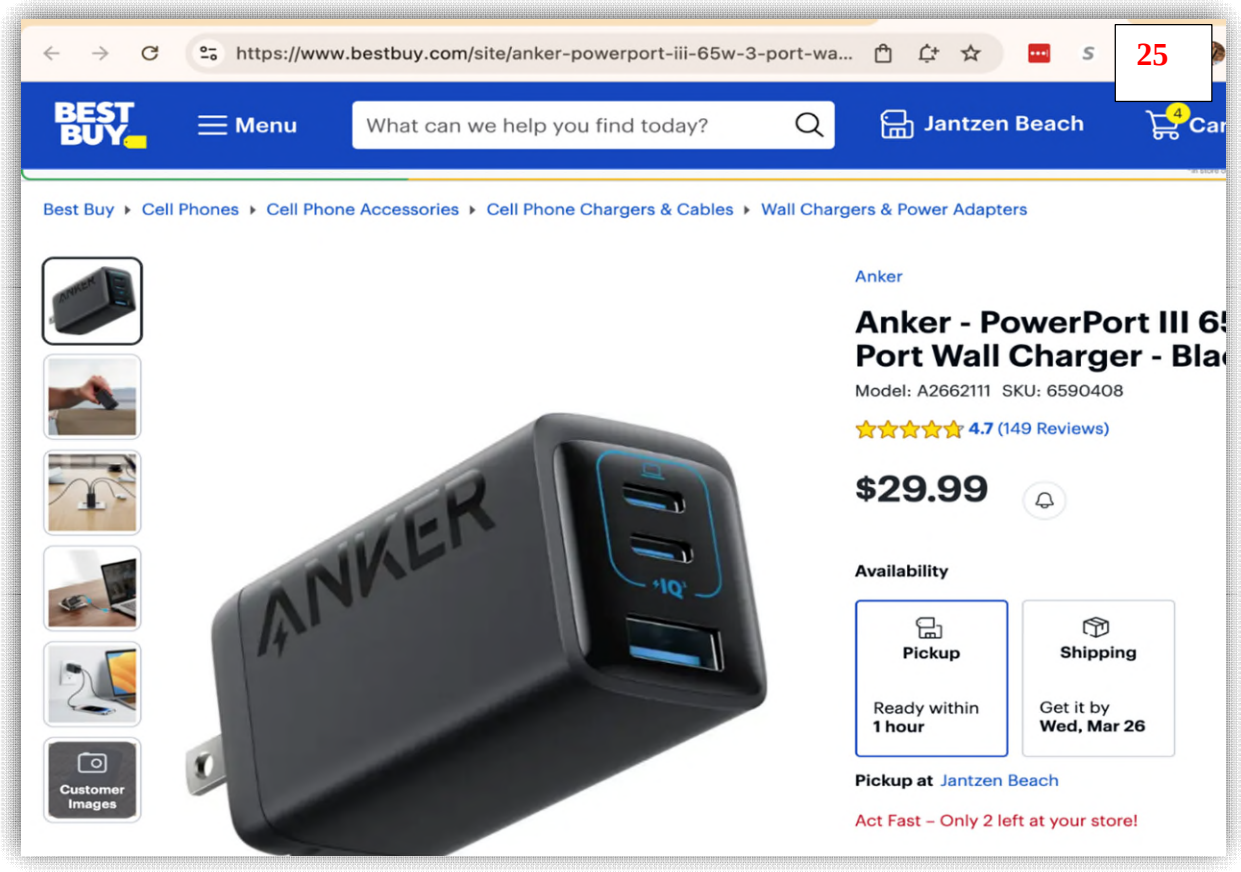
Image 24 (below): In the cookies stored on the buyer's browser from the moment that the buyer lands on the Best Buy webpage after clicking on the Just Josh affiliate link, all the way through checkout and post-checkout, a cookie called "partner" indicates that the referrer for the sale is Howl Technologies, which references the third-party affiliate platform through which Just Josh generated the link.




89. Indeed, for a purchase made by the buyer on March 20, 2025, at or around 3:55pm EST, Just Josh earned a commission for the transaction depicted above for the purchase of an Apple Power Adapter from Best Buy.

90. In scenario two—where a buyer *does* engage with the Capital One Shopping browser extension—when the buyer clicks on Just Josh's affiliate link for Best Buy and lands on the Best Buy webpage, Just Josh's affiliate tracking code is stored in the buyer's browser. But when the buyer reaches the checkout page and engages with the Capital One Shopping browser extension, Just Josh's affiliate tracking code is displaced when Capital One artificially simulates a referral click, tricking the buyer's browser into treating Capital One as the referrer of the sale and inserting Capital One's affiliate tracking code in the browser. As a result, even though Just Josh is entitled to earn a commission for referring the sale to Best Buy, Josh Josh is ultimately deprived of that commission, and Capital One earns the commission instead.

Image 25 (below): The buyer follows a Just Josh affiliate link to Best Buy and intends to purchase this Anker Port Wall Charger.



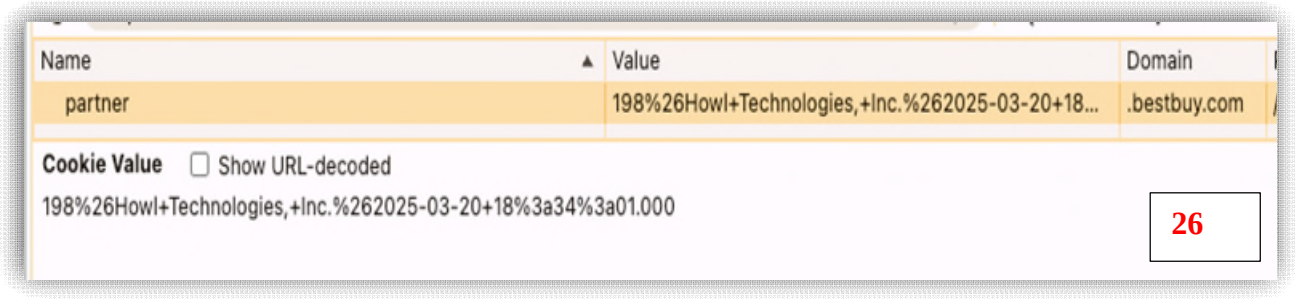
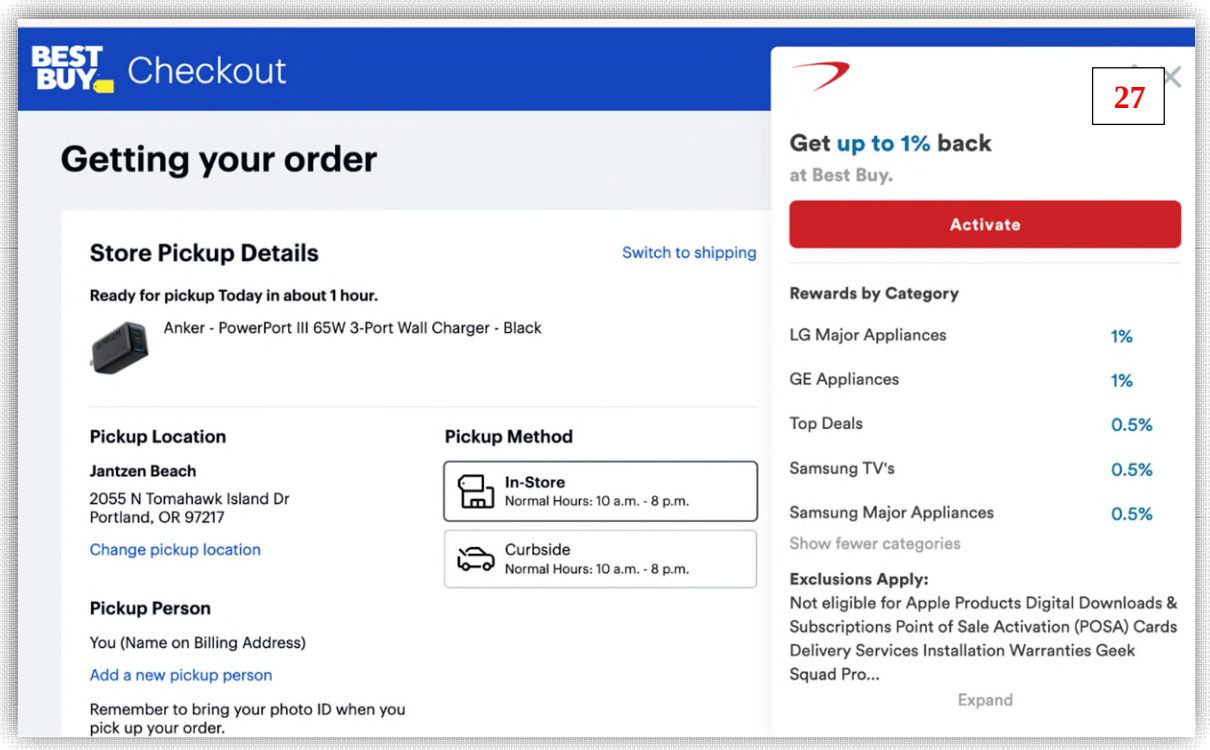




Image 26 (above): After the buyer lands on the Best Buy merchant webpage, and until the buyer engages with the Capital One Shopping browser extension, the buyer's browser stores affiliate code identifying Just Josh as the referrer of any sale made by that buyer on Best Buy's webpage, using Just Josh's affiliate identifier through the third-party affiliate marketing platform "Howl."

Image 27 (below): On the checkout page, the buyer chooses to engage with the Capital One Shopping browser extension and accept Capital One's offer to "Activate" cash back.



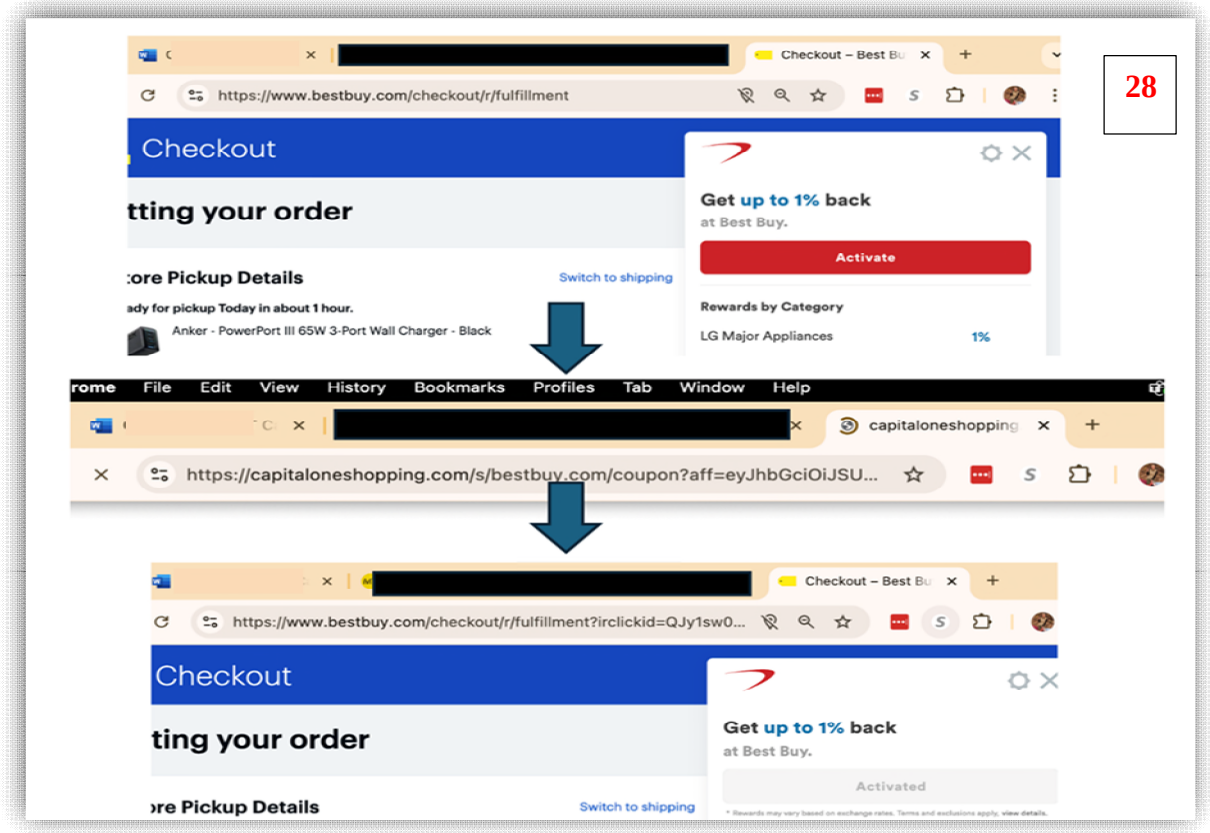



Image 28 (above): As soon as the buyer elects to "Activate" rewards in the Capital One Shopping browser extension, the extension forces a refresh of the buyer's Best Buy checkout page, simulating a referral click by the buyer to Best Buy, and injecting Capital One Shopping's affiliate tracking code in place of Just Josh's affiliate tracking code. The extension then directs the buyer back onto the very same Best Buy checkout page that the buyer was already on, all without the lay consumer knowing any such swap occurred.

Image 29 (below): In the cookies stored on the buyer's browser after the buyer engages with the Capital One Shopping browser extension on the checkout page of Best Buy, the cookie called "partner" identifies Capital One as the referrer for the sale even though the buyer was only ever referred to Best Buy by Just Josh, using Just Josh's affiliate link.

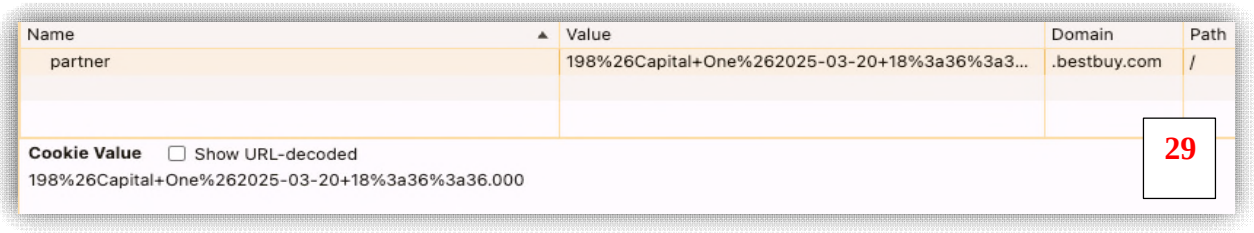
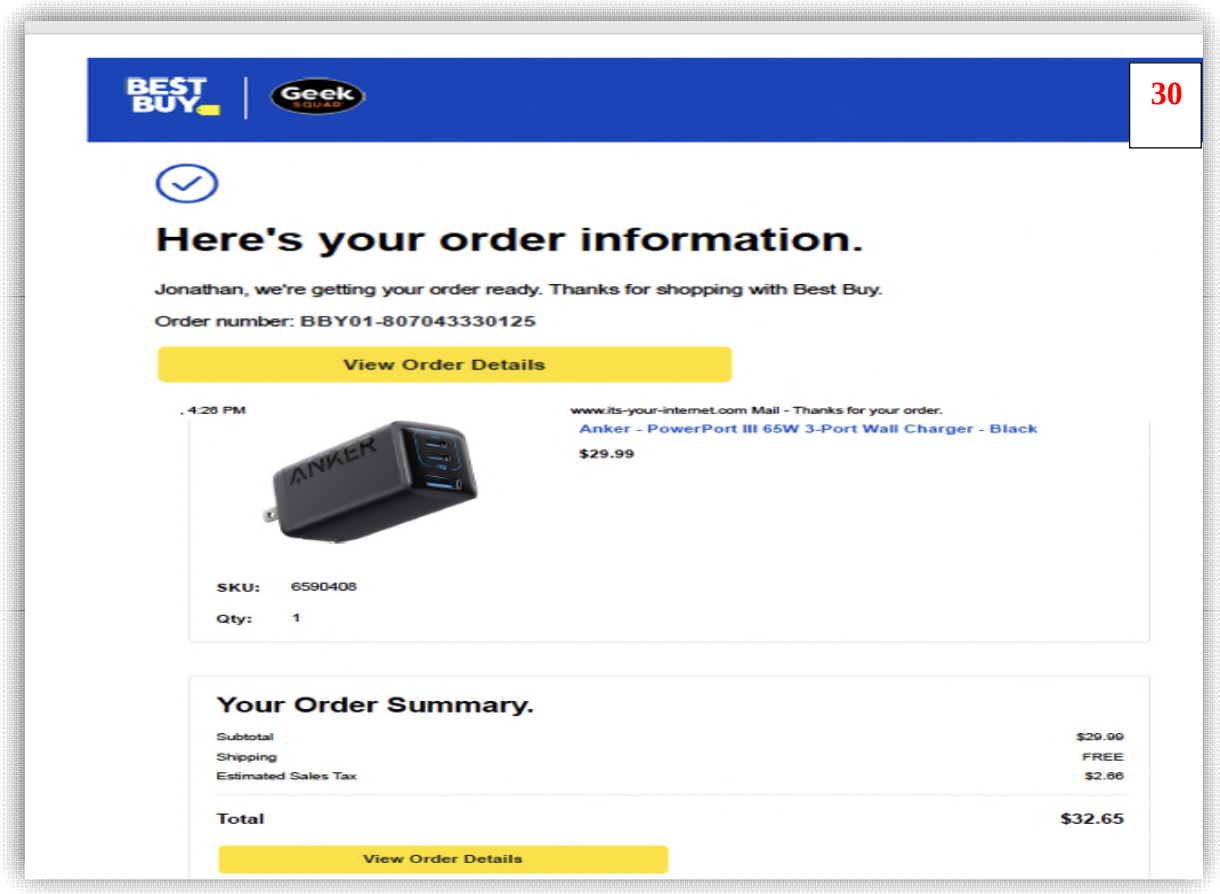



Image 30: The buyer completes the purchase described in the images above.



91. In this second scenario, in which the buyer purchased the Anker Port WallCharger by clicking on Just Josh's affiliate link on March 20, 2025, at or around 4:10pm ET, Just Josh *did not* see or receive any commission. In other words, even though Plaintiff Just Josh was entitled to receive a commission on this transaction, he did not receive it.

92. As depicted above, by analyzing a consumer's network traffic while using the Capital One Shopping browser extension one can see how a consumer's web browser, a given website, and other third parties interact. Importantly, this network traffic is typically invisible to ordinary website users.

93. By reviewing this network traffic, one can see that how the Capital One Shopping browser extension invisibly replaces affiliate code in the cookies on the consumer's computing device that would otherwise credit the rightful salesperson—the creator—with the sale of that particular product or service.

94. Capital One thus gets credit for the referral and ultimate purchase of the product even though it did not, at any point, refer the user to the merchant's page.

### 7. The Technology Powering Capital One Shopping's Theft of Affiliate Commissions

95. Capital One's bait-and-switch is not an outlier; it is a well-known deceptive practice known as "cookie-stuffing."

96. Capital One entices consumers to activate the Capital One Shopping browser extension in several different ways, each of which displaces the rightful referrer and steals commission credit for sales that Capital One did not influence, much less generate.

97. Going under the "hood" of a consumer's browser and the Capital One Shopping browser extension itself makes it clear that the Capital One Shopping browser extension is forcing the consumer's browser to refresh a merchant's webpage, artificially simulating a new, external

referral click putatively referring that consumer to the merchant's webpage, even though the user was already on the merchant's webpage all along. The purpose of this is to surreptitiously replace creators' affiliate codes with codes that credit Capital One with any referral and ultimately with commission on the sale.

98. The images below illustrate what happens when a consumer wants to purchase a product or service that a specific creator is promoting by clicking on that creator's affiliate link and proceeding to the online merchant's website to complete the checkout process. In this scenario, the buyer[33] already has the Capital One Shopping browser extension installed.


Image 31: The buyer navigates from Plaintiff ToastyBros YouTube Video to the online merchant Newegg's website by clicking on ToastyBros' affiliate marketing link.

99. As shown above, the buyer who has installed the Capital One Shopping browser extension navigated to Newegg.com—which was being promoted by creator and Plaintiff

[33] As to this particular transaction, the buyer was an expert retained by Plaintiffs.

ToastyBros—by clicking on the ToastyBros' affiliate marketing link.

100. The image above shows the online merchant's website "markup," which is what ordinary website visitors see, and the image below shows the inspection panel, which provides a glimpse into what is happening behind the scenes in the Capital One Shopping browser extension. More specifically, it shows that Capital One is recording ToastyBros' affiliate URL for Newegg.com that the buyer clicked on.

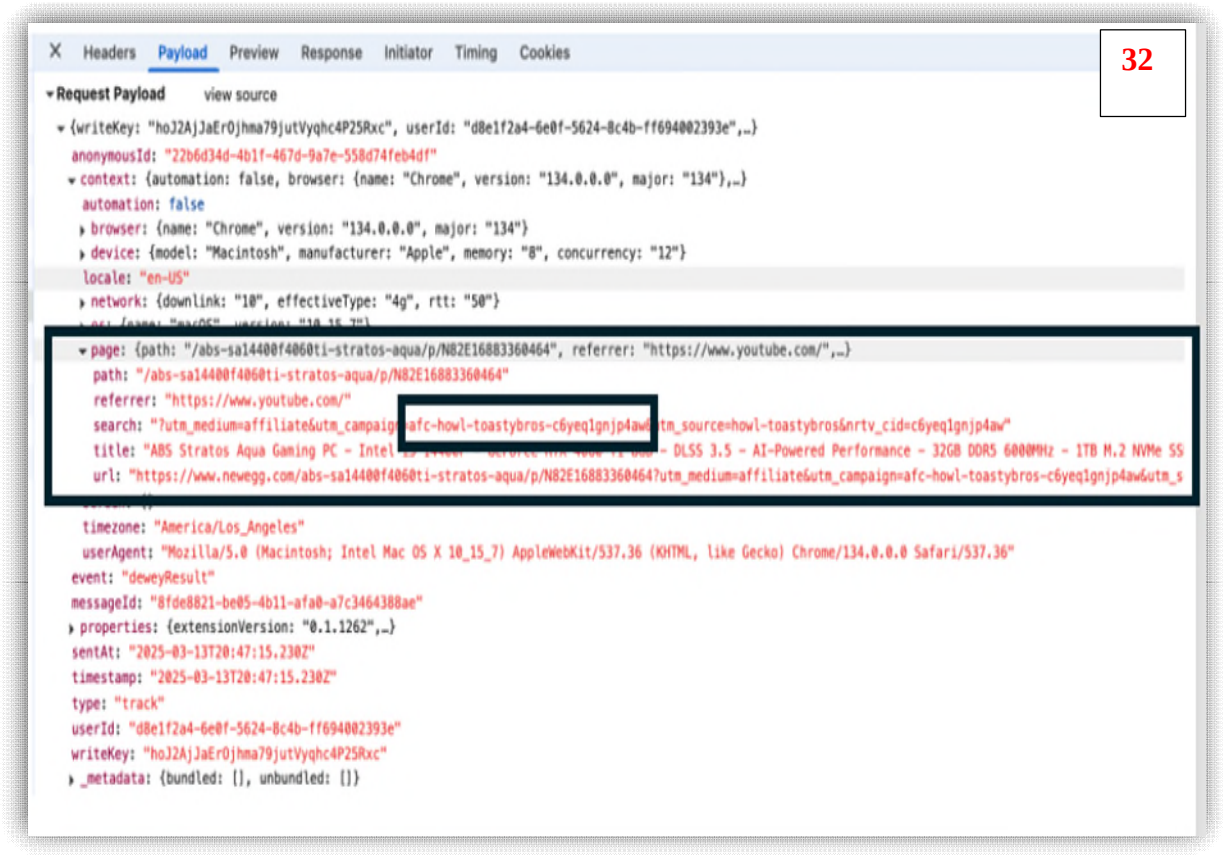



Image [32]: Behind the scenes, the Capital One Shopping browser extension tracks a record of ToastyBros' referral of the buyer to Newegg's merchant webpage.

101. Next, the buyer adds an item to their cart and proceeds to the checkout page. At this

point, the browser extension pops up automatically to notify the buyer of potentially applicable coupon codes.

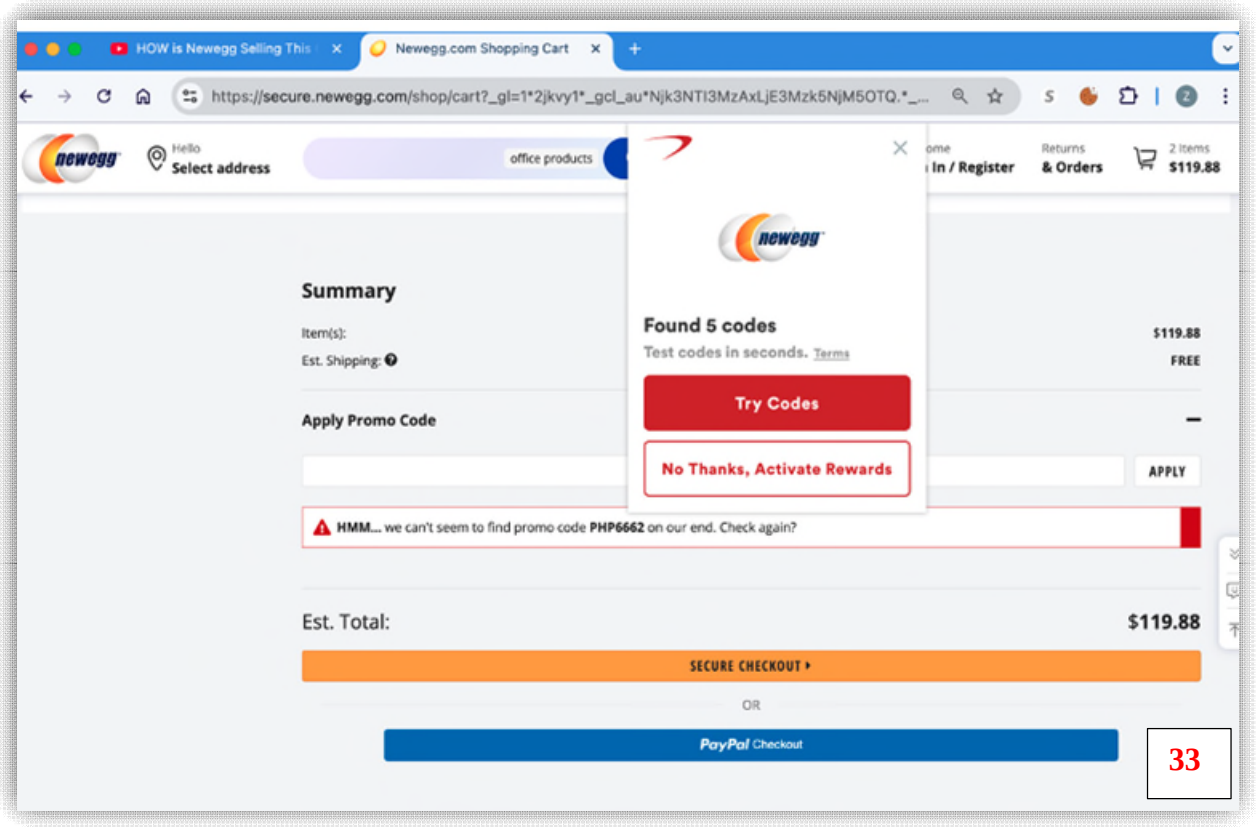



Image 33: After following Plaintiff ToastyBros' affiliate link to Newegg.com, the buyer with the Capital One Shopping browser extension lands on the Newegg checkout page, and sees a pop-up inviting the buyer to either "try" coupon codes or "activate rewards."

102. Here, the buyer clicks the "Try Codes" button, triggering two separate and simultaneous actions on the Capital One Shopping browser extension, as captured in the images below: (1) on the main product page where the buyer has engaged the extension to test the 5 coupon codes it has located, the extension attempts to apply each of those coupon codes in the "Apply Promo Code" box on the checkout page, and (2) the extension opens a second mini tab of the merchant's checkout page which is unnoticeable to the lay consumer and on which the extension forces a refresh of the main tab, simulating a click by the buyer on a second affiliate link attributed

to Capital One, despite the fact that the buyer never left the merchant's webpage and never clicked on any Capital One affiliate link. This simulated click tricks the browser into behaving as though the buyer clicked on a second, intervening affiliate link after using Plaintiff ToastyBros' affiliate link to navigate to the Newegg merchant webpage. In doing so, Capital One displaces any affiliate code from ToastyBros and replaces it with Capital One's affiliate code that credits Capital One with the referral and facilitates Capital One's receipt of any commission earned on the product sale.

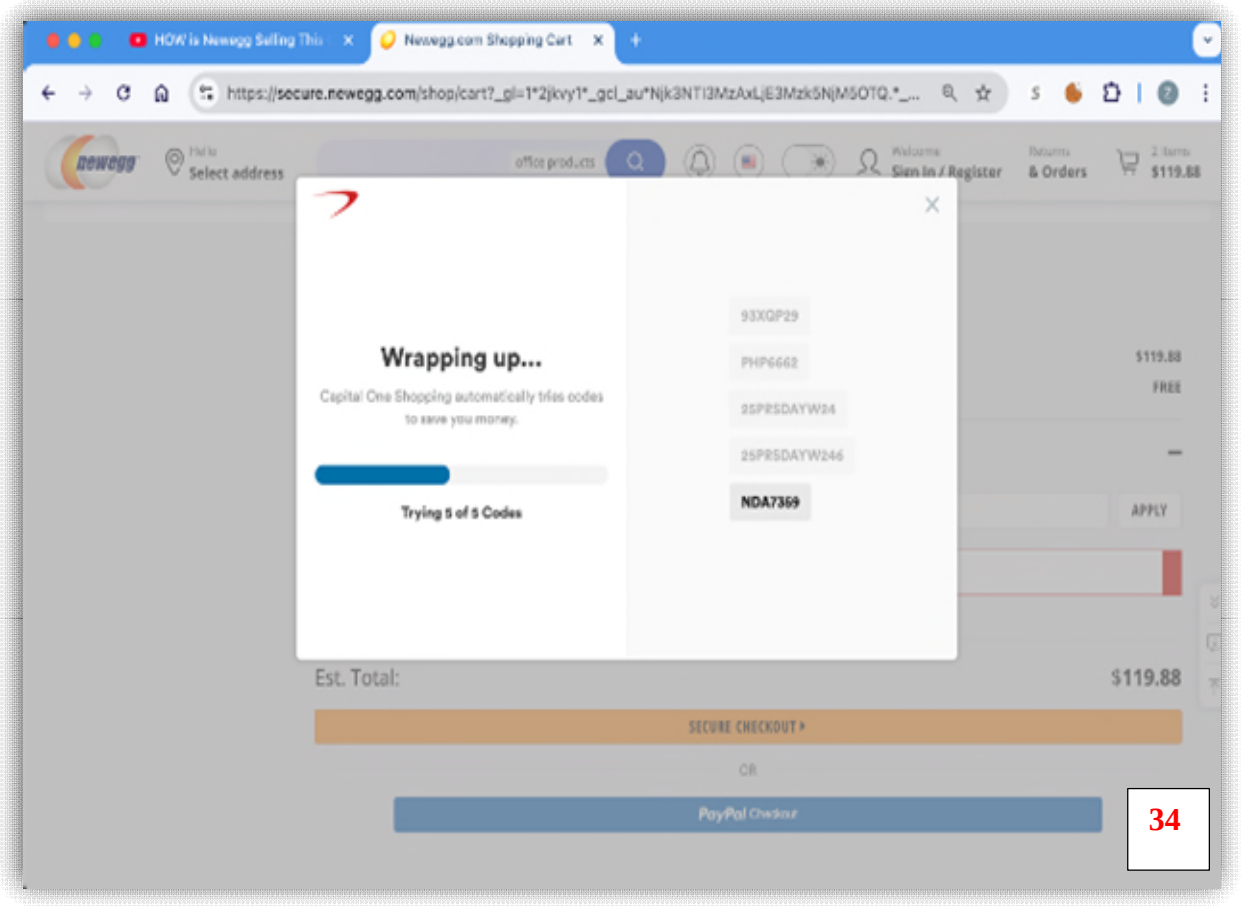



Image 34: On the main tab, the buyer watches the Capital One Shopping browser extension test various coupon codes on the Newegg merchant's checkout page.

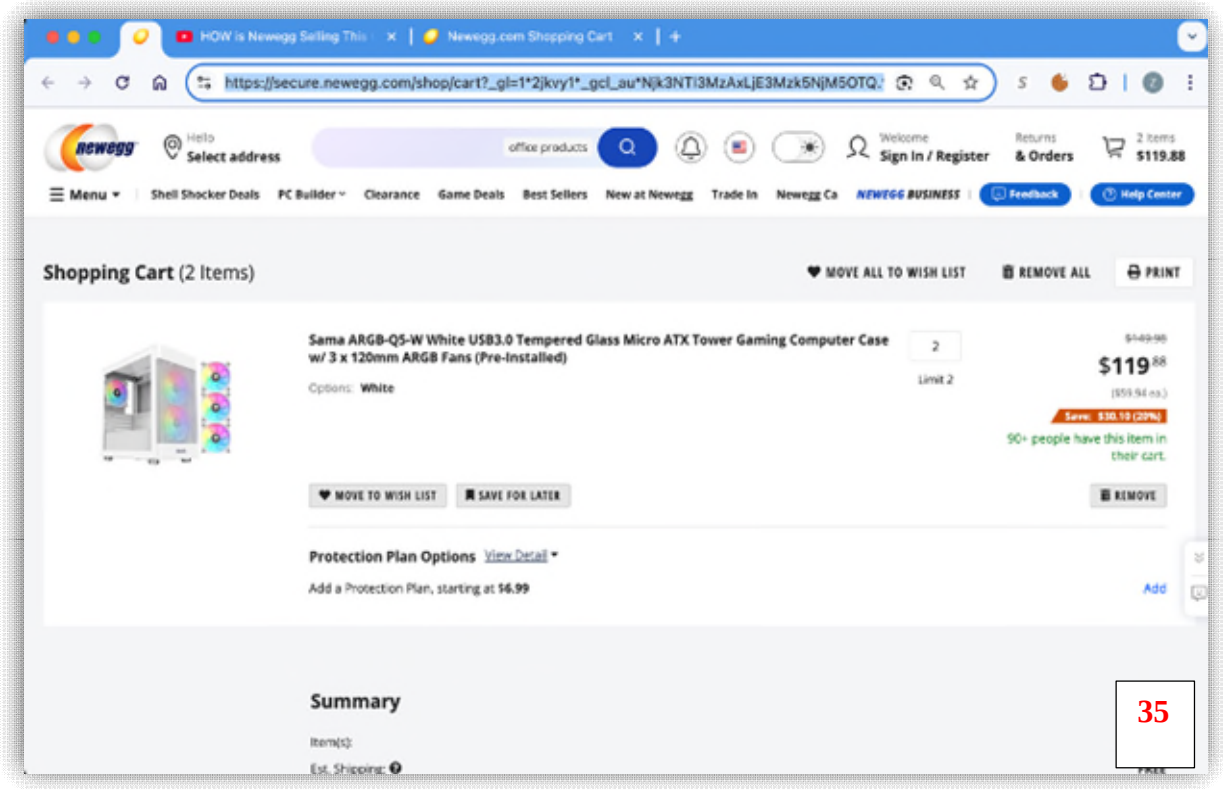



Image 35 (above): On a second mini-tab, invisible to the consumer, the Capital One Shopping browser extension reopens the Newegg checkout page, but does not attempt to apply any coupon codes. Instead, on the mini-tab, the extension injects code into the merchant's URL that forces a refresh of the main checkout page, simulating the buyer clicking on a Capital One affiliate link.

Image 36 (below): The Capital One Shopping browser extension injects a type of code called "JSON" into the URL on the mini-tab that forces a redirect to the merchant's page via a simulated click on a Capital One affiliate link.

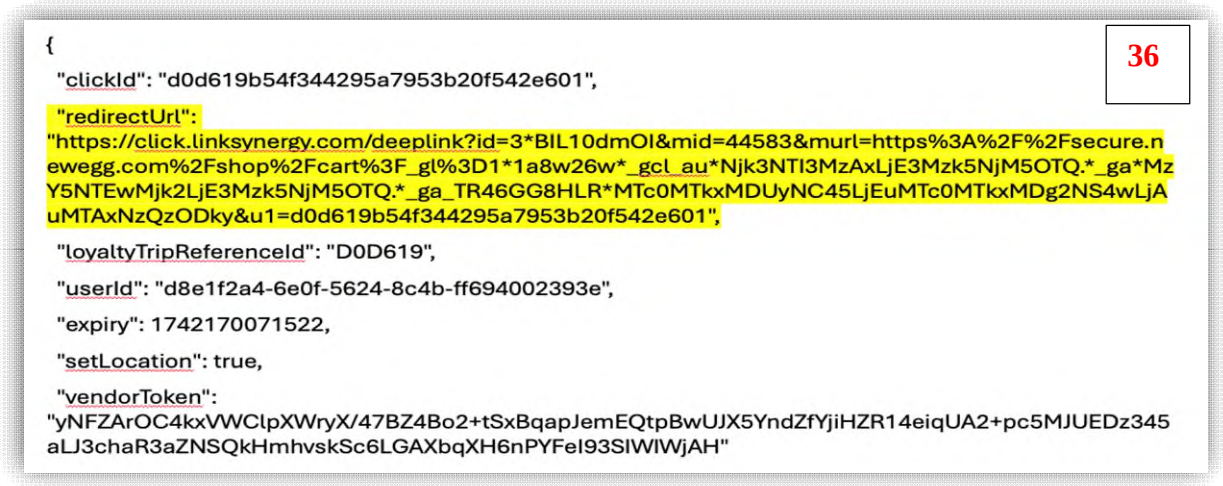


Image 37: This image depicts the URL that the Capital One extension opened in the mini-tab. After the browser completes the redirect to the URL injected by the extension, the mini-tab's URL for the merchant's checkout page contains an affiliate code attributing Capital One as the affiliate and referral source. The UTM (or "Urchin Tracking Module")[34] parameters in the URL allow Newegg to track the performance of affiliate marketing campaigns and understand which affiliates and links are driving traffic and conversions. Now those UTM parameters identify Capital One as being responsible for referring the buyer to Newegg's webpage, even though the buyer was already on Newegg's webpage after following the ToastyBros affiliate link, and never left the Newegg page or clicked on an intervening affiliate link.


103. Capital One's tactics are not novel. This scheme is known as "cookie stuffing." Cookie stuffing is a fraudulent affiliate marketing technique in which "the Web cookies used to determine the likely source of user traffic are overwritten without the user's knowledge."[35]

104. As one academic research paper described the scheme:

> [I]nstead of using the affiliate URL as a clickable link, a fraudulent affiliate may cause the browser to directly fetch her affiliate URL on a page controlled by her without any explicit clicks from the user, thereby tricking the affiliate program into returning a cookie that then identifies the fraudulent affiliate as the referrer for the user's transactions. As a result, not only does an affiliate program pay a non-advertising affiliate, but the fraudulent cookie overwrites any existing affiliate cookie that may have already been present, thereby potentially stealing the commission from a legitimate affiliate. Furthermore, cookie-stuffing fraud is typically completely opaque to an end user and goes against the advertising guidelines issued by the Federal Trade Commission for marketers, which require

[34]UpPromote, *Add UTM parameters to affiliate link*, https://docs.uppromote.com/settings/affiliate-link-settings/add-utm-to-affiliate-link (last visited Mar. 24, 2025).

[35] Neha Chachra, et al., *Affiliate Crookies: Characterizing Affiliate Marketing Abuse*, 1 (2015), https://www.sysnet.ucsd.edu/~voelker/pubs/crookies-imc15.pdf.

declaration of any financial relationship with advertisers.[36]

105. Cybersecurity companies such as McAfee classify extensions that attempt to commit improper cookie stuffing as "malicious code" because they attempt to alter cookies that they are not authorized to alter.[37]

106. Capital One Shopping engages in precisely this conduct. Without any explicit clicks from a user on a Capital One affiliate link, Capital One's Extension forces the consumer's browser to refresh a merchant's webpage, *simulating* a referral click from the consumer on a Capital One Shopping affiliate link even when the consumer never clicked on any such link. While the consumer may have clicked to engage the extension to search for and test coupon codes or activate any shopping rewards, the consumer is unaware of the fact that engaging with the extension will cause the consumer's browser to surreptitiously refresh a merchant's webpage, thereby overwriting a creator's affiliate cookies with a Capital One affiliate cookie. The consumer is further unaware of the fact that these engagements with the extension will cause the merchant to identify Capital One as the referrer—or "last click"—for the consumer's transactions. This allows Capital One to steal the commission from the creator who actually referred the consumer to the merchant's webpage to make a purchase.

### 8. In Addition to Capital One's Own Logs, Capital One's Conduct Is Also Traceable Via Statistical Analysis

107. As discussed in Section IV.A.6 above, Capital One receives logs of all the instances in which the Capital One Shopping Extension replaces the referring tracking codes with its own. But, even in the absence of these logs, there is sound statistical evidence showing that for affiliates

[36] *Id.* at 2.
[37] McAfee Labs, *Malicious Cookie Stuffing Chrome Extensions with 1.4 Million Users*, McAfee (Aug. 29, 2022), https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malicious-cookie-stuffing-chrome-extensions-with-1-4-million-users/.

with at least 50 purchases on which they were eligible to receive a commission, it is a near statistical certainty that Capital One stole at least one of those commissions by overwriting tracking codes through the Capital One Shopping browser extension.

108. Plaintiffs' expert conducted a statistical analysis using the Monte Carlo simulation. The Monte Carlo simulation functions like series of weighted coin flips, and allows for the use of limited (here, publicly available) data to determine the probability of that an event occurred in the absence of discovery.[38]

109. In this analysis, the expert ran a Monte Carlo simulation for sets of 1000 affiliates, across a variety of scenarios such as the number of purchases, that took into consideration variables like the size of the internet audience, the relative proportions of global vs. US-based purchasing activity, internet browser prevalence (e.g., Chrome, Firefox, Edge, and Safari) and coupon extension prevalence (e.g., Honey, Capital One Shopping, and Microsoft), to calculate the likelihood that, given a legitimate affiliate purchase, Capital One stole the creator's commission. Plaintiffs' expert tested scenarios exploring various probabilities that Capital One stole affiliate commissions.

110. This analysis reveals that for affiliates with as few as 50 purchases on which they are eligible to receive a commission there is a 95.3% likelihood that at least one (and as many as 7) of their commissions have been stolen by Capital One specifically (*see* Figure 1, below). This means that when the simulation ran, 953 times out of 1000 at least one commission was stolen by

[38] Monte Carlo simulations, and similar statistical techniques, are used routinely in real world applications and have been accepted by courts. For instance, in *Lyondell Chemical Co. v. Occidental Chemical Corp*., 608 F.3d 284 (5th Cir. 2010), which involved environmental cleanup costs, the Monte Carlo method successfully withstood a *Daubert* challenge, with the court concluding that the Monte Carlo method of statistical analysis, as employed to measure probability of various outcomes when reaching exact numerical result is impossible or infeasible and when data provides known range, was reliable. *Id*. at 293.

Capital One specifically. When the number of purchases reached 100, there was a 99.8% likelihood that at least one (and as many as 15) of the commissions were stolen by Capital One specifically (*see* Figure 1, below).

111. Plaintiffs believe discovery will show that, when the Capital One Shopping browser extension is activated, it always swaps the affiliate codes (as shown in the exemplars above), on partner merchant sites. To account for the prospect that, instead, the Capital One Shopping browser extension replaces the affiliate tracking code with its own tracking code less than 100% of the time, Plaintiffs' expert also performed a sensitivity analysis, testing scenarios in which Capital One Shopping overwrites the tracking code only 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, and 90% of the time (shown in Figure 1 below, in the "Swap Probability" column). The results show that even when the probability that Capital One replaces the tracking code with its own is only 50%, an affiliate with as few as 100 purchases, which would otherwise receive a commission, has a 97% likelihood of having at least one (and as many as 10) of their commissions stolen by Capital One (*see* Figure 1 supra). Moreover, where the probability that Capital One replaces the tracking code with its own is merely 10%, an affiliate with 500 purchases, which would otherwise receive a commission, has a 96% likelihood of having at least one (and as many as 11) of their commissions stolen by Capital One (*see* Figure 1, below).

**Figure 1: Statistical Probability that Capital One Stole At Least One Purchase Commission via Monte Carlo Simulation – Sensitivity Analysis**

| Affiliate Purchases | Swap Probability | Affected Probability | Num Affected (Mean) | Num Affected (SD) |
|---|---|---|---|---|
| 50 | 10% | 29.1% | 0.34 | 0.58 |
| 50 | 20% | 48.6% | 0.66 | 0.81 |
| 50 | 30% | 63.4% | 1.00 | 0.99 |
| 50 | 40% | 73.1% | 1.29 | 1.13 |
| 50 | 50% | 81.5% | 1.68 | 1.28 |
| 50 | 60% | 85.6% | 2.02 | 1.41 |
| 50 | 70% | 90.5% | 2.32 | 1.48 |
| 50 | 80% | 94.2% | 2.77 | 1.55 |
| 50 | 90% | 95.7% | 2.94 | 1.62 |
| **50** | **100%** | **95.3%** | 3.29 | 1.77 |
| 100 | 10% | 51.4% | 0.69 | 0.80 |
| 100 | 20% | 73.1% | 1.32 | 1.16 |
| 100 | 30% | 86.9% | 2.05 | 1.43 |
| 100 | 40% | 93.9% | 2.64 | 1.55 |
| **100** | **50%** | **97.0%** | 3.28 | 1.76 |
| 100 | 60% | 98.7% | 3.96 | 1.92 |
| 100 | 70% | 99.2% | 4.66 | 2.09 |
| 100 | 80% | 99.5% | 5.37 | 2.23 |
| 100 | 90% | 99.8% | 5.94 | 2.32 |
| **100** | **100%** | **99.8%** | 6.58 | 2.51 |
| **500** | **10%** | **96.0%** | 3.32 | 1.79 |
| 500 | 20% | 100.0% | 6.54 | 2.48 |
| 500 | 30% | 100.0% | 9.92 | 3.05 |
| 500 | 40% | 100.0% | 13.31 | 3.55 |
| 500 | 50% | 100.0% | 16.49 | 4.03 |
| 500 | 60% | 100.0% | 20.12 | 4.64 |
| 500 | 70% | 100.0% | 23.02 | 4.78 |
| 500 | 80% | 100.0% | 26.57 | 4.96 |
| 500 | 90% | 100.0% | 29.75 | 5.30 |
| 500 | 100% | 100.0% | 32.95 | 5.57 |

**B. Plaintiffs' Experiences**

112. **Ahntourage Media LLC**[39] reviews "all things chairs" and home office technology on his YouTube channel and other social media platforms. Ahntourage Media began this work in 2019 and has since produced and posted 230 YouTube videos and has 88,400 subscribers to his YouTube channel.

113. Ahntourage Media has always relied on affiliate marketing links posted on his social media platforms to earn commissions for sales he generates and to help pay for the time and effort that Ahntourage Media puts into producing its content. Last year alone, Ahntourage Media earned approximately $400,000 through affiliate marketing.

114. Ahntourage Media partners with a number of merchants that also partner with Capital One, including, but not limited to, Andaseat, Branch Furniture, Colamy, Herman Miller, Razer, SIHOO, Staples, and Steelcase.

115. There have been at least 500 customer purchases using Ahntourage Media's affiliate links, on which Ahntourage Media was eligible to receive a commission from a merchant. Ahntourage Media, for example, generated at least 291 individual sales from Herman Miller alone in 2024, all of which were sales on which Ahntourage Media was eligible to receive a commission.

116. Ahntourage Media has been conducting affiliate marketing for Razer for six years and expects to continue partnering with Razer in the future.

117. Ahntourage Media has been conducting affiliate marketing for Herman Miller and Staples for five years and expects to continue partnering with Herman Miller and Staples in the

[39] Ahntourage Media's social media handles include @Ahnestly (YouTube), @StayAhnest (Instagram), @StayAhnest (X), @StayAhnest (TikTok), and Ahnestly (Facebook).

future.

118. Ahntourage Media has been conducting affiliate marketing for Steelcase for four years and expects to continue partnering with Steelcase in the future.

119. Ahntourage Media has been conducting affiliate marketing for Andaseat, Branch Furniture, and SIHOO for three years and expects to continue partnering with Andaseat, Branch Furniture, and SIHOO in the future.

120. Ahntourage Media has been conducting affiliate marketing for Colamy for one year and expects to continue partnering with Colamy in the future.

121. When Capital One Shopping artificially replaces Ahntourage Media's affiliate tracking code with Capital One's tracking code, Ahntourage Media is deprived of referral fees and sales commissions to which it was rightfully entitled. Ahntourage Media would have earned more in commissions but for Capital One's scheme to poach commissions via its Capital One Shopping browser extension. Through this extension, Capital One stole credit for sales that Ahntourage Media generated with its affiliate links.

122. **Just Josh, Inc.**,[40] has worked since 2019 to review electronic products and provide valuable content to viewers through his YouTube channel and website. Just Josh has produced and posted over 300 YouTube videos and boasts 303,000 subscribers to its channel. In November 2024, Just Josh's website received at least 64,000 visitors.

123. Just Josh has relied on affiliate marketing links on his YouTube channel and website since Just Josh's inception to earn commissions and help pay for the company's time and effort.

[40] Just Josh's social media handles include @JustJoshTech (YouTube), @JustJoshBusiness (YouTube), @justjosh.life (Instagram), @JustJoshLife (X), and @justjoshtech (TikTok).

124. Just Josh partners with a number of merchants that also partner with Capital One, including, but not limited to, Best Buy, Dell, HP, Lenovo, Samsung, and Walmart. There have been at least 500 customer purchases using Just Josh's affiliate links, on which Just Josh was eligible to receive a commission from a merchant.

125. Just Josh has been working with these merchants for a number of years and expects the business relationships to continue.

126. Just Josh has spent substantial time and money developing a community of viewers that support it and reviewing the products for which it provides affiliate links. In November 2024, Just Josh received approximately $50,000 in affiliate link revenue.

127. When Capital One Shopping artificially replaces Just Josh's affiliate tracking code with Capital One's code, Just Josh is deprived of referral fees and sales commissions to which it was rightfully entitled. Just Josh would have earned more in commissions but for Capital One's scheme to poach commissions via its Capital One Shopping browser extension. Through this extension, Capital One stole credit for sales that Just Josh generated with its affiliate links.

128. **Storm Productions LLC ("Madison Avenue Spy")**[41] has operated a popular shopping blog that showcases the best deals in the fashion world via affiliate links since 2008.[42] The blog has approximately 22,000 subscribers and generates significant traffic. Madison Avenue Spy also runs an Instagram account by the same name and a Substack called MadSpy, where she also regularly posts fashion affiliate links. The Instagram account has over 112,000 followers, and the Substack has over 11,000 subscribers. In addition to these platforms, Madison Avenue Spy has

[41] Madison Avenue Spy's social media handles include @madisonavenuespy (Instagram), @madisonavenuespy (Threads), @MadisonAveSpy (X), @madspy (Substack), and @madisonavenuespy (TikTok).
[42] https://madisonavenuespy.com/.

an online presence on Pinterest, TikTok, X (formerly Twitter), Facebook, and Telegram.

129. Madison Avenue Spy invests substantial time and effort cultivating her follower base, searching for the best fashion deals from online merchants, and promoting those deals online. Madison Avenue Spy partners with online merchants, either directly or through third-party affiliate networks, to advertise their products through affiliate links. Madison Avenue Spy directly influences millions of dollars in retail sales every year.

130. For years, Madison Avenue Spy has earned substantial commissions on sales generated via affiliate links. In the past year, Madison Avenue Spy has earned over $200,000 in affiliate link revenue.

131. Madison Avenue Spy works with a number of prominent online merchants that also partner with Capital One, including, but not limited to, Bloomingdale's, Gap, Neiman Marcus, Nordstrom, the Outnet, Saks Fifth Avenue, and Target. There have been at least 500 customer purchases using Madison Avenue Spy's affiliate links, on which Madison Avenue Spy was eligible to receive a commission from a merchant.

132. Madison Avenue Spy has conducted affiliate marketing for Bloomingdales, Gap, Neiman Marcus, Nordstrom, The Outnet, and Saks Fifth Avenue for ten or more years. Madison Avenue Spy has already conducted affiliate marketing for all of these merchants in 2025 and expects to continue partnering with these merchants on affiliate marketing in the future.

133. Madison Avenue Spy has conducted affiliate marketing for Target for seven years. Although Storm Productions has not yet partnered with Target in the first three months of 2025, Storm Productions expects to continue partnering with Target on affiliate marketing in the future.

134. When Capital One Shopping artificially replaces Madison Avenue Spy's affiliate tracking code with Capital One's code, Madison Avenue Spy is deprived of referral fees and sales

commissions to which it was rightfully entitled. Madison Avenue Spy would have earned more in commissions but for Capital One's scheme to poach commissions via its Capital One Shopping browser extension. Through this extension, Capital One stole credit for sales that Madison Avenue Spy generated with her affiliate links.

135. **TechSource Official**[43] operates a YouTube channel that has over 3.9 million followers. TechSource is dedicated to technology-related content, focusing on PC hardware reviews, custom PC builds, gaming and workstation setups and makeovers, and reviews on a wide range of tech products. TechSource regularly partners with online merchants either directly or through third-party affiliate networks, to promote products on his YouTube channel and to drive sales through affiliate links.

136. TechSource has devoted tremendous effort and time to building its YouTube channel and continuously devotes time and effort to researching new products before deciding whether to promote them on its platform.

137. In 2024, TechSource earned approximately $105,000 in affiliate marketing revenue.

138. TechSource works with a number of prominent online merchants that also partner with Capital One, including, but not limited to, Newegg (through Rakuten) and eBay. There have been at least 500 customer purchases using TechSource's affiliate links, on which Tech Source was eligible to receive a commission from a merchant.

139. TechSource has been conducting affiliate marketing for Newegg and eBay for at least five years and expects to continue to partner with Newegg and eBay on affiliate marketing in

[43] TechSource's social media handles include @TechSource (YouTube), @ed.techsource (Instagram) @ed.techsource (Threads), @EdTechSource (X), @techsource_official (TikTok), and TechSource Club (Discord).

the future.

140. Over the past several years, TechSource has noticed that the revenue from its commissions has dropped despite its viewership having increased during the same period of time.

141. When Capital One Shopping artificially replaces TechSource's affiliate tracking code with Capital One's code, TechSource is deprived of referral fees and sales commissions to which it was rightfully entitled. TechSource would have earned more in commissions but for Capital One's scheme to poach commissions via its Capital One Shopping browser extension. Through this extension, Capital One stole credit for sales that TechSource generated with its affiliate links.

142. **ToastyBros, LLC**,[44] operates a popular YouTube channel called Toasty Bros, as well as several other social media channels.

143. The Toasty Bros YouTube channel has approximately over 790,000 followers. It is a tech-oriented channel that offers PC hardware reviews and provides custom PC build guides. The other channels operated by ToastyBros are a mix of hobbyist channels and gaming focused channels and have a total of approximately 140,000 followers.

144. ToastyBros invests substantial time and effort into researching and trying out hardware, appliances, and tools that ToastyBros promotes, and finding the best deals from online merchants. ToastyBros relies on affiliate links that it posts on its YouTube channel pages, as well as their Instagram, Twitter, and TikTok accounts, to earn commissions and help pay for their time and effort.

[44] ToastyBros, LLC's social media handles include @ToastyBros (YouTube), @ToastyDIY (YouTube), @ToastyBrosClips (YouTube), @toastybros (Instagram), @toastybrostech (Instagram), @ToastyBrosTech (X), @toastydeals (X), @toastybros (Threads), @toastybrosofficial (TikTok), @toastybros (Twitch), Toasty Bros (Discord).

145. ToastyBros regularly partners with affiliate market networks to promote products for online merchants and occasionally partners directly with online merchants. ToastyBros posts affiliate links on all its channels and generates commission revenue by directing followers of its channels to online merchants' websites.

146. ToastyBros earns approximately $280,000 in affiliate link marketing revenue per year.

147. ToastyBros works with a number of prominent online merchants that also partner with Capital One, including, but not limited to, AliExpress, Best Buy, Newegg, and Walmart. There have been at least 500 customer purchases using ToastyBros' affiliate links, on which ToastyBros was eligible to receive a commission from a merchant.

148. ToastyBros has been conducting affiliate marketing for AliExpress for nine years and expects to continue partnering with AliExpress on affiliate marketing in the future.

149. ToastyBros has been conducting affiliate marketing for Best Buy, Newegg, and Walmart for five years and expects to continue partnering with these merchants on affiliate marketing in the future.

150. When Capital One Shopping artificially replaces ToastyBros' affiliate tracking code with Capital One's code, ToastyBros is deprived of referral fees and sales commissions to which it was rightfully entitled. ToastyBros would have earned more in commissions but for Capital One's scheme to poach commissions via its Capital One Shopping browser extension. Through this extension, Capital One stole credit for sales that ToastyBros generated with its affiliate links.

**C. Damages & Harm**

151. Plaintiffs and Class members were harmed by Capital One's conduct because the

Capital One Shopping browser extension systematically steals commission payments from their rightful owners—i.e., the individual who promoted and shared the affiliate link and generated the referral and ultimate sale of a product or service.

152. Plaintiffs were harmed by Capital One, via the Capital One Shopping browser extension, which deprived them of referral fees and sales commissions to which they are rightfully entitled as the generator of those referrals and sales.

153. The Capital One Shopping browser extension is activated during millions of online purchases each year. In the absence of the Capital One Shopping browser extension, Plaintiffs and Class members would have earned more money in the form of referral fees and sales commissions from their respective affiliate links.

154. Plaintiffs continue to devote time and energy to content creation to generate commissions. Plaintiffs accordingly face future harm in the form of stolen referral fees and sales commissions because the Capital One Shopping browser extension continues to steal affiliate marketing commissions with each passing day.

## V. CLASS ALLEGATIONS

155. Plaintiffs, on behalf of themselves and as a class action under the Federal Rules of Civil Procedure, Rule 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), seek damages and injunctive relief on behalf of the members of the following Class and constituent Subclasses (collectively, the "Class"):

> **Nationwide Class:** All persons in the United States who participated in an affiliate commission program with a United States online merchant and had commissions diverted to Capital One as a result of the Capital One Shopping browser extension.
>
> **California Subclass:** All members of the Class who reside in California.
>
> **Pennsylvania Subclass:** All members of the Class who reside in

Pennsylvania.

**New York Subclass:** All members of the Class who reside in New York.

156. The California, Pennsylvania, and New York Subclasses are referred to hereinafter collectively as "the State Subclasses."

157. Excluded from the Class are the Defendants and their officers, directors, management, employees, subsidiaries, or affiliates. Also excluded are the district judge or magistrate judge to whom this case is assigned, as well as those judges' immediate family members, judicial officers and their personnel, and all governmental entities.

158. **Numerosity:** Members of the Class are so numerous that joinder is impracticable. There are at least tens of thousands of members of the Class, geographically dispersed throughout the United States, such that joinder of all Class members is impracticable. There are at least thousands of members of each Subclass, such that joinder of all Subclass members is likewise impracticable.

159. **Typicality:** Plaintiffs' claims are typical of the claims of the other Class members. The factual and legal bases of Defendants' liability are the same and resulted in injury to Plaintiffs and all other members of the Class.

160. **Adequate representation:** Plaintiffs will represent and protect the interests of the Class both fairly and adequately. They have retained counsel who are competent and experienced in complex class-action litigation. Plaintiffs have no interests that are antagonistic to those of the Class, and their interests do not conflict with the interests of the Class members whom they seek to represent.

161. **Commonality and Predominance:** Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class members

because Defendants have acted on grounds generally applicable to the Class and because Class members share a common injury. Thus, determining damages with respect to the Class as a whole is appropriate. Defendants' wrongful conduct was the same as to all Class members, causing class members common injuries.

162. There are common questions of law and fact specific to the Class that predominate over any questions affecting individual members, including:

a. Whether Defendants programmed and designed the Capital One Shopping browser extension in a manner that wrongfully credits Capital One as the originator of sales referrals;

b. Whether the scheme described herein results in Capital One being awarded commission payments that it did not rightfully earn;

c. Whether Capital One was unjustly enriched to the detriment of Plaintiffs in the form of commission payments;

d. Whether Defendants, through the actions alleged in this complaint, interfered with Plaintiffs' prospective business advantage;

e. Whether Defendants, through the actions alleged in this complaint, interfered with Plaintiffs' contractual relations;

f. Whether Defendants, through the actions alleged in this complaint, violated consumer protection laws in the states of the California, New York, and Pennsylvania Subclasses;

g. Whether Defendants, through the actions alleged in this complaint, violated federal and state computer fraud and abuse laws;

h. Whether consumers and Class members have been damaged by Defendants'

conduct; and

i. The nature and scope of appropriate injunctive relief.

163. **Superiority:** Class proceedings on these facts are superior to all other available methods for the fair and efficient adjudication of this controversy, given that joinder of all members is impracticable. Even if members of the Class could sustain individual litigation, that course would not be preferable to a class action because individual litigation would increase the delay and expense to the parties due to the complex factual and legal controversies present in this matter. Here, the class action device will present far fewer management difficulties, and it will provide the benefit of a single adjudication, economies of scale, and comprehensive supervision by this Court. Further, uniformity of decisions will be ensured.

164. **Ascertainability:** Class treatment is appropriate as membership in the Class can be determined through Defendants' business records. Ascertainment of the Class through Defendants' business is both economically and administratively feasible.

165. Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants;
- The prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;

- Defendants have acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole; and
- The claims of Class members are comprised of common issues whose resolution in a class trial would materially advance this litigation.

153. All applicable statute(s) of limitations have been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and Class members could not have reasonably discovered Defendants' practice of surreptitiously manipulating network transmissions and altering Plaintiffs and Class members' cookie data to allow Capital One to take credit for sales commissions it did not earn.

154. Defendants were and remain under a continuing duty to disclose to Plaintiffs and Class members their practice of displacing tracking codes that point to creators as the source of a referral and substituting their own tracking codes to appropriate commissions that belong to creators like Plaintiffs and Class members. As a result of the active concealment by Defendants, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

155. Plaintiffs make the following specific fraud allegations with as much specificity as possible, although they do not have access to information necessarily available only to Defendants.

156. **Who**: Defendants knew of and actively concealed their practice of affiliate commission diversion through cookie stuffing using the Capital One Shopping browser extension.

157. **What**: Defendants knew that, as described above, consumers' activation of the Capital One Shopping extension diverts referral commissions from creators to Defendants by surreptitiously overwriting the tracking codes with Capital One's own data, thereby crediting the

consumer's purchase to Capital One and not the referring creator. Capital One's extension is designed to continuously upload detailed logs to Capital One's server at track.capitaloneshopping.com, contemporaneously with a consumer's browsing. These logs include, among other detailed information, the full-string URL of each web page visited by a consumer. From these full-string URLs, Capital One knew when a consumer navigated to a specific merchant's website from a specific affiliate. Capital One's browser extension is also designed to inject a hidden tab, which redirects a consumer's browser to a purpose-built URL, to overwrite the previous tracking code with its own. Capital One knew that when the extension injected a hidden tab after a consumer visited a merchant's website from an affiliate link, it would interfere with the commission of that affiliate.

158. **When**: Defendants concealed their commission diversion scheme and Capital One Shopping's cookie-stuffing functionality from Class members at all times.

159. **Where**: Defendants concealed their commission diversion scheme and Capital One Shopping extension's cookie-stuffing functionality from Class members by failing to disclose it on their website, advertisements to the public, the applicable terms of service or privacy policy, or in any information that is disclosed to consumers who install the extension in the ordinary course.

160. **Why**: Defendants concealed their commission diversion scheme and Capital One Shopping extension's cookie-stuffing functionality for the purpose of inducing consumers to install the Capital One Shopping extension so that Defendants could surreptitiously use consumers' computers to overwrite Class members' tracking codes and steal commissions rightfully earned by those Class members.

## VII. CAUSES OF ACTION

### FIRST CAUSE OF ACTION

### UNJUST ENRICHMENT
### (UNDER VIRGINIA LAW OR THE APPLICABLE LAW OF EACH PLAINTIFF'S HOME STATE)

161. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

162. Plaintiffs lack an adequate remedy at law.

163. Plaintiffs and Class members have an interest, both equitable and legal, in the referral fees and commission payments to which they were wrongfully deprived. These payments were rightfully earned by Plaintiffs and Class members, not Capital One.

164. Plaintiffs and Class members conferred a benefit on Capital One, because Plaintiffs and Class members drove prospective customers to the merchants' web pages, through their marketing and influencing efforts, and their affiliate links, to make a purchase that resulted in Capital One's receipt of (stolen) referral fees and commission payments.

165. Capital One knew that it was receiving Plaintiffs' and Class members' referral fees and commission payments because the Capital One browser extension code is designed to monitor for other tracking codes contained in the browsing history URL. Specifically, Capital One's extension is designed to continuously upload detailed logs to Capital One's server at track.capitaloneshopping.com contemporaneously with a consumer's browsing. These logs include, among other detailed information, the full-string URL of each web page visited by a consumer. From these full-string URLs, Capital One knew when a consumer navigated to a specific merchant's website from a specific affiliate. Capital One's browser extension is also designed to inject a hidden tab, which redirects a consumer's browser to a purpose-built URL, to

overwrite the previous tracking code with its own. Capital One knew that when the extension injected a hidden tab after a consumer visited a merchant's website from an affiliate link, it would interfere with the commission of that affiliate.

166. Capital One should have reasonably expected to repay those referral fees and commission payments to Plaintiffs and Class members, because Capital One knows that creators are entitled to commissions for driving traffic to merchants. Indeed, Capital One itself pays affiliates in other contexts. Capital One pays affiliates for driving traffic to its site for credit cards[45] and driving traffic to download its Capital One Shopping browser extension.[46]

167. But for Capital One's unjust and improper use of the browser extension it would not have been credited and awarded commission on sales that emanated from Plaintiffs' and Class members' respective affiliate marketing links.

168. As a result of Capital One's wrongful conduct as alleged in this Complaint, it has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members.

169. Capital One continues to benefit and profit from Plaintiffs' and Class members directing prospective customers to the merchants' web pages through their marketing and influencing efforts and their affiliate links, and driving them to make a purchase which results in Capital One's receipt of (stolen) referral fees and commission payments, while Plaintiffs and Class members continue to have their rightful commission payments diverted to Capital One.

170. Capital One's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including by using the Capital One Shopping browser extension to wrongfully credit itself with referrals and commissions it did not rightfully earn.

[45] https://tapfiliate.com/blog/credit-card-affiliate-programs/
[46] https://www.performcb.com/agency/clients/capital-one-shopping-affiliate-program/

171. The benefit conferred upon, received, and enjoyed by Capital One was not conferred officiously or gratuitously, and it would be inequitable and unjust for Capital One to retain the benefit.

172. Equity and good conscience militate against permitting Capital One to retain the profits and benefits from its wrongful conduct, which should be restored to Plaintiffs and Class members.

## SECOND CAUSE OF ACTION

## INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE (UNDER VIRGINIA LAW OR THE APPLICABLE LAW OF EACH PLAINTIFF'S HOME STATE)

173. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein

174. Plaintiffs and Class members are engaged in an economic relationship with online merchants, including but not limited to Best Buy, Lenovo, Samsung, Walmart, Bloomingdale's, Gap, Neiman Marcus, Nordstrom, the Outnet, Saks Fifth Avenue, and Target, by referring their followers to those merchants through affiliate links. In return, online merchants provide Plaintiffs and Class members with referral fees or commissions. These relationships are ongoing, and Plaintiffs and Class members plaintiffs are reasonably certain that their business expectancy with online merchants will continue in the form of referral links and commissions, based on the length and extent of the parties' relationships.

175. Capital One had knowledge of the facts that should lead to disclosure of the existence of business relationships between Plaintiffs and Class members, under which Plaintiffs and Class members receive commissions from online merchants via affiliate links under a last-click-attribution model, because Capital One specifically designed its browser extension to

monitor for and replace creators' tracking codes with its own tracking codes, and based on Capital One's knowledge about industry practices in general, where online merchants work with affiliate marketers. Capital One's extension is designed to continuously upload detailed logs to Capital One's server at track.capitaloneshopping.com contemporaneously with a consumer's browsing. These logs include, among other detailed information, the full-string URL of each web page visited by a consumer. From these full-string URLs, Capital One knew when a consumer navigated to a specific merchant's website from a specific affiliate. Capital One's browser extension is also designed to inject a hidden tab, which redirects a consumer's browser to a purpose-built URL, to overwrite the previous tracking code with its own. Capital One knew that when the extension injected a hidden tab after a consumer visited a merchant's website from an affiliate link, it would interfere with the commission of that affiliate.

176. Through use of the Capital One Shopping browser extension, Capital One steals commission payments from Plaintiffs and Class members who promoted and shared an affiliate link and generated the referral and ultimate sale of an online merchant's product or service. Specifically, Capital One overwrites tracking codes that identify creators as the source of the referral, substitutes its own tracking codes, and holds itself out as the referrer of the specific products and/or services even though the sale in question emanated from a creator's affiliate marketing link. This conduct, which interferes with Plaintiffs' and Class members' prospective economic advantage, is improper because it circumvents industry norms around last-click attribution, and because it independently constitutes intentional interference with contractual relations, conversion, and violations of the Computer Fraud and Abuse Act, New York's General Business Law, Pennsylvania's Computer Offenses Law, and California's Computer Data Access and Fraud Act.

177. Capital One either intended to usurp commissions from Plaintiffs and Class members through the conduct alleged herein or knew that its conduct would appropriate commissions and referral fees.

178. Plaintiffs and Class members were harmed by Capital One's conduct because the Capital One Shopping browser extension caused the online merchants to breach their contracts with Plaintiffs and Class members by paying Capital One, instead of Plaintiffs and Class members, the monies that they rightfully earned as the true originators of sales arising from their affiliate marketing links.

179. As discussed above, including in paragraphs 50 through 150, absent Capital One's conduct, Plaintiffs and Class members would have received from merchants the commissions they should have earned from referrals through their affiliate links .

180. As a result of the above conduct, Capital One is liable to Plaintiffs and Class members for damages in an amount to be determined at trial.

## THIRD CAUSE OF ACTION

## INTENTIONAL INTERFERENCE WITH CONTRACTUAL RELATIONS (UNDER VIRGINIA LAW OR THE APPLICABLE LAW OF EACH PLAINTIFF'S HOME STATE)

181. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

182. Plaintiffs and Class members have ongoing, valid, and enforceable contractual agreements with online merchants to promote products and services in exchange for commissions. These include, but are not limited to, contracts with Best Buy, Lenovo, Samsung, Walmart, Bloomingdale's, Gap, Neiman Marcus, Nordstrom, the Outnet, Saks Fifth Avenue, and Target. Under the provisions of these contracts, Plaintiffs and Class members are entitled to earn a

commission for every purchase by an online shopper where the shopper made the purchase after navigating to the site using an affiliate link distributed by Plaintiffs and Class members.

183. Capital One had knowledge of the facts that should lead to disclosure of the existence of contracts between Plaintiffs and Class members, under which Plaintiffs and Class members receive commissions from online merchants via affiliate links under a last-click-attribution model, because Capital One specifically designed its browser extension to monitor for and replace creators' tracking codes with its own tracking codes, and based on Capital One's knowledge about industry practices in general, where online merchants work with affiliate marketers. Capital One's extension is designed to continuously upload detailed logs to Capital One's server at track.capitaloneshopping.com contemporaneously with a consumer's browsing. These logs include, among other detailed information, the full-string URL of each web page visited by a consumer. From these full-string URLs, Capital One knew when a consumer navigated to a specific merchant's website from a specific affiliate. Capital One's browser extension is also designed to inject a hidden tab, which redirects a consumer's browser to a purpose-built URL, to overwrite the previous tracking code with its own. Capital One knew that when the extension injected a hidden tab after a consumer visited a merchant's website from an affiliate link, it would interfere with the commission of that affiliate.

184. Capital One knew that its tracking-code-overwriting conduct was certain or substantially certain to interfere with Plaintiffs' and Class members' contracts with merchants, such that merchants would breach their contracts with Plaintiffs and Class members by paying Capital One, instead of Plaintiffs and Class members, the monies that they rightfully earned as the true originators of sales arising from their affiliate marketing links.

185. Capital One intentionally disrupted this contractual relationship by intentionally

replacing the tracking codes associated with Plaintiffs' and Class members' affiliate links with tracking codes associated with Capital One. Capital One's conduct caused merchants to breach their contracts with Plaintiffs and Class members by paying Capital One, instead of Plaintiffs and Class members, the monies that Plaintiffs and Class members rightfully earned as the true originators of sales arising from their affiliate marketing links.

186. Because Plaintiffs and Class members were deprived of their rightfully earned commissions, they sustained harm and economic injury as a direct and proximate result of Capital One's tortious interference with contractual relations. Plaintiffs and Class members accordingly seek damages in an amount to be proven at trial, as well as injunctive relief barring further interference.

## FOURTH CAUSE OF ACTION

### CONVERSION
### (UNDER VIRGINIA LAW OR THE APPLICABLE LAW OF EACH PLAINTIFF'S HOME STATE)

187. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

188. At the time consumers made purchases on merchants' websites, Plaintiffs and Class members had a right to possess the tracking code that identified Plaintiffs and Class members as the parties to whom merchants should pay commissions for referring consumers to products and services sold by the merchants. These tracking codes are specific to each Plaintiffs and Class member.

189. Capital One wrongfully exercised control over the Plaintiffs' and Class members' affiliate codes by intentionally causing the tracking codes to be overwritten with Capital One's tracking codes, thus depriving Plaintiffs and Class members of their tracking codes.

190. Capital One's wrongful exercise of control over Plaintiffs' and Class members' tracking codes constitutes conversion.

191. As a direct and proximate result of Capital One's conversion, Plaintiffs and Class members were harmed.

192. Capital One is liable to Plaintiffs and Class members for damages and costs permitted by law.

## FIFTH CAUSE OF ACTION

## VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT 18 U.S.C. § 1030, *ET SEQ.* (ON BEHALF OF THE CLASS)

193. Plaintiffs re-allege and incorporate by reference all factual allegations above as if fully set forth herein.

194. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, makes it unlawful to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access, and by means of such conduct further[] the intended fraud and obtain[] anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period." 18 U.S.C. § 1030(a)(4).

195. 18 U.S.C. § 1030(g) provides a private right of action to "[a]ny person who suffers damage or loss by reason of a violation of this section[.]"

196. Through its browser extension, Capital One, knowingly and with intent to defraud, exceeded its authorized access to the browsers and computers of consumers that downloaded its browser extension, and through this conduct furthered its fraudulent scheme to wrongfully obtain the affiliate commissions of Plaintiffs and Class members.

197. Capital One exceeded its authorized access to the computers of its consumers by accessing and altering or removing tracking codes that Capital One was not entitled to access and alter or remove. Capital One exceeded its authorized access by circumventing the technical restrictions in place.

198. As described above, when a consumer activates the Capital One extension, Capital One extension's code surreptitiously injects a new, hidden browser tab in the background to avoid detection by the consumer. This hidden tab redirects the consumer's browser to a purpose-built URL. Capital One then artificially mimics a genuine click on an affiliate marketing link associated with its own affiliate marketing account in this hidden browser tab, causing the online merchant's website to replace the tracking codes of Plaintiffs and Class members with Capital One's tracking codes.

199. Merchants (and affiliate networks) restrict Capital One's ability to overwrite the tracking codes directly, because Capital One would not get paid a commission if it performed this overwriting directly. Capital One only gets the commission if it causes the tracking code to be overwritten through an indirect approach: a forced redirect to another website or a hidden tab opening.

200. Consumers of Capital One Shopping did not grant Capital One access that is necessary to be able to alter tracking codes because consumers themselves do not have that access and cannot overwrite tracking codes. From a browser's settings, an ordinary computer owner can see the fact that tracking codes are installed and can delete them. But an ordinary computer owner cannot access and overwrite the tracking codes. One would need specialized "developer tools" or other specialized software to access and overwrite tracking codes.

201. Lacking permission to access and alter the tracking codes, Capital One had to use

the sophisticated technique described above to circumvent the technical restrictions in place to allow Capital One Shopping to artificially "trick" the consumer's browser and the online merchant's website into replacing the legitimate tracking codes of Plaintiffs and Class members with Capital One's illegitimate tracking codes.

202. Consumers of Capital One Shopping do not expect the Capital One Shopping extension to operate in this manner or to alter this data, and the extension's cookie-stuffing functionality is not disclosed in the applicable terms of service or privacy policy, or in any information that is disclosed to consumers who install the extension in the ordinary course.

203. Capital One Shopping's code is executed in the browsers of computers that are used in or affect interstate commerce, and thus meet the definition of "protected computer" under the CFAA.

204. Capital One's substitution of its own tracking codes for the tracking codes of Plaintiffs and Class members impairs the integrity and availability of the data contained in the original affiliate cookies designating Plaintiffs and Class members as the proper party to receive an affiliate commission. Capital One's cookie stuffing disrupted the commission attribution process, including communications between the merchant website and the merchant servers that attributed the sale to a Class member instead of Capital One. As a result of this interruption of service, Plaintiffs and Class members have lost substantial revenue from these valuable commissions that were improperly diverted to Capital One. Thus, Plaintiffs and Class members have suffered damages and loss well in excess of $5,000 during a year within the relevant period as a result of Capital One's conduct.

205. Plaintiffs and the Class seek compensatory damages, injunctive relief, and all other legal or equitable relief available under the CFAA.

## SIXTH CAUSE OF ACTION

### VIOLATION OF THE NEW YORK DECEPTIVE PRACTICES ACT N.Y. GEN. BUS. LAW § 349 (ON BEHALF OF PLAINTIFF STORM PRODUCTIONS LLC, AND THE NEW YORK SUBCLASS)

206. Plaintiff Storm Productions LLC re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

207. Under the New York Deceptive Practices Act, it is unlawful to use deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

208. The New York Deceptive Practices Act also provides that "…any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such actions."

209. Plaintiff Storm Productions and the members of the New York Subclass are considered "persons" for the purpose of the Act.

210. Capital One's acts, omissions, practices, and nondisclosures as alleged in this complaint constitute unlawful deceptive acts or practices within the meaning of the Act.

211. Capital One engaged in consumer-oriented conduct by directing their deceptive acts and practices to the consuming public and the marketplace, such that it has broader impact on consumers at large, impacting the consumer decision-making process.

212. Capital One takes unfair advantage of the affiliate marketing attribution system and the consumers who are entitled to a competitive market. Consumers often follow or subscribe to the content and marketing and promotional material affiliates create. Consumers click on affiliate links to make purchases from a merchant based on the built-up trust and goodwill between

consumers and affiliates regarding the quality of the products that the affiliates are promoting. Capital One, through its covert tracking-code overwriting conduct, steals commissions from affiliates, harming them economically and, thereby, pushing them out of the market. Because affiliates are pushed out of the market, consumers lose options in the marketplace and their decision-making process is affected.

213. Capital One's acts or practices were deceptive and misleading in a material way. Capital One's actions of surreptitiously overwriting creators' tracking codes with its own tracking codes are likely to mislead others as to the identity of the affiliate who is entitled to receive a commission in connection with a sale.

214. Plaintiff Storm Productions and members of the New York Subclass suffered an injury as a result of Capital One's deception. Capital One covertly replaced their tracking codes with its own to divert their commissions to itself, with no corresponding benefit to Plaintiff Storm Productions or the members of the New York Subclass. And because the Capital One Shopping extension acted in a covert manner, Plaintiff Storm Productions and members of the New York Subclass could not have avoided the harm.

215. As a direct and proximate result of Capital One's wrongful conduct, Plaintiff Storm Productions and members of the New York Subclass have suffered damages, including lost affiliate commissions that rightfully belonged to them. The full extent of the damages is not yet fully known and continues to impact Plaintiff Storm Productions and members of the New York Subclass.

216. There is a causal relationship between Plaintiff Storm Productions' and New York Subclass members' loss and Capital One's actions and practices. But for Capital One's deceptive acts and practices, Plaintiff Storm Productions and members of the New York Subclass would not

have had their commissions diverted to Capital One.

217. At all relevant times, Capital One was willfully and knowingly engaged in the use of an unfair, unlawful, and deceptive practice or act.

## SEVENTH CAUSE OF ACTION

## VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *ET SEQ.* (ON BEHALF OF PLAINTIFF TECHSOURCE OFFICIAL AND THE CALIFORNIA SUBCLASS)

218. Plaintiff TechSource Official ("California Plaintiff") re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

219. The California Plaintiff lacks an adequate remedy at law.

220. California's Unfair Competition Law (UCL) defines "unfair competition" to include any "unlawful, unfair, or fraudulent" business act or practice. Cal. Bus. & Prof. Code § 17200 *et seq.*

221. Capital One has engaged in acts and practices that are unfair in violation of the UCL.

222. Capital One is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

223. Capital One committed unfair business practices by using the Capital One Shopping browser extension to steal credit for sales referrals on purchases made in the state of California, and thereby received commission payments that rightfully belonged to California Plaintiff and members of the California Subclass.

224. Capital One's conduct is unfair in violation of the UCL because it violates California's public policy against interfering with another's prospective economic advantage. *See* 5 Witkin, Summary 11th Torts § 854 (2024).

225. Capital One's conduct is unlawful because it constitutes conversion, interference

with prospective economic advantage, interference with contractual relations, and violations of the Computer Fraud and Abuse Act, New York's General Business Law, California's Computer Data Access and Fraud Act.

226. Capital One wrongfully deprives California Plaintiff and Subclass members of monies they rightfully earned as the true originators of sales arising from affiliate marketing links.

227. The gravity of harm resulting from Capital One's practice of appropriating commissions that belong to creators like California Plaintiff and Subclass members outweighs any potential utility therefrom. Capital One's conduct set forth in this Complaint violates public policy and is unscrupulous, offensive, and substantially injurious.

228. Capital One actually and proximately caused harm to California Plaintiff and Subclass members in that, among other things, they suffered economic injury by being deprived of commissions they should have earned from referrals through their affiliate links.

229. The conduct alleged herein is continuing and there is no indication that Capital One will cease such activity in the future.

230. Capital One's conduct in violation of the UCL has caused California Plaintiff and members of the California Subclass to be deprived of referral fees and commission payments for sales they rightfully originated. California Plaintiff and the members of the California Subclass thus suffered lost money or property as a result of Capital One's conduct.

231. California Plaintiff therefore seeks restitution, an injunction, and all other appropriate relief in equity, including reasonable attorneys' fees and costs of suit.

## EIGHTH CAUSE OF ACTION

### CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS & FRAUD ACT CAL. PENAL CODE § 502 (ON BEHALF OF PLAINTIFF TECHSOURCE OFFICIAL AND THE CALIFORNIA SUBCLASS)

232. The California Plaintiff re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

233. The California Comprehensive Computer Data Access & Fraud Act (CDAFA), Cal. Penal Code § 502, makes it unlawful to:

> (1) Knowingly access[] and without permission alter[], damage[], delete[], destroy[], or otherwise use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. . . .
>
> (4) Knowingly access[] and without permission add[], alter[], damage[], delete[], or destroy[] any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. . . .
>
> (8) Knowingly introduce[] any computer contaminant into any computer, computer system, or computer network.

234. Through its browser extension, Capital One knowingly accesses and without permission alters, damages, deletes, and/or destroys the tracking code data of California Plaintiff and California Subclass members, in order to both (a) execute its unlawful and fraudulent scheme and (b) wrongfully control or obtain money, property, or data through the diversion of affiliate commissions that rightfully belong to California Plaintiff and California Subclass members.

235. Through its browser extension, Capital One knowingly accesses and without permission adds, alters, damages, deletes, and/or destroys the tracking code data of California

Plaintiff and California Subclass members, which resides on covered computer systems.

236. Under CDAFA, a "computer contaminant" is "any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information." Cal. Penal Code § 502(b)(12).

237. California Plaintiff and California Subclass members have an ownership interest in the tracking code data that is modified, damaged, and/or destroyed by the Capital One Shopping extension. The Capital One Shopping extension contains computer instructions that are designed to modify, damage, and/or destroy the tracking code data of California Plaintiff and California Subclass members without their intent or permission, thus meeting the definition of "computer contaminant" under CDAFA. Capital One knowingly introduces this computer contaminant into the computers of consumers of its browser extension in violation of CDAFA.

238. Capital One did not request or receive permission from either the consumers of its browser extension or California Plaintiff and California Subclass members to add, alter, damage, delete, or destroy the tracking code data of California Plaintiff and California Subclass members residing on consumers' browsers, nor did Capital One request or receive permission to divert the affiliate commissions of California Plaintiff and California Subclass members to Capital One. Consumers of Capital One Shopping did not grant Capital One access that is necessary to be able to alter tracking codes because consumers themselves do not have that access and cannot overwrite tracking codes. From a browser's settings, an ordinary computer owner can see the fact that tracking codes are installed and can delete them. But an ordinary computer owner cannot access and overwrite them. One would need specialized "developer tools" or other specialized software to access and overwrite tracking codes.

239. Lacking permission to access and alter the tracking codes, Capital One circumvented technical barriers that are in place to restrict access and alteration of tracking code data. As described above, when a consumer activates the Capital One Shopping extension, Capital One extension's code surreptitiously injects a new, hidden browser tab in the background to avoid detection by the consumer. This hidden tab redirects the consumer's browser to a purpose-built URL. Capital One then artificially mimics a genuine click on an affiliate marketing link associated with its own affiliate marketing account in this hidden browser tab, causing the online merchant's website to replace the tracking codes of Plaintiffs and the Class with Capital One's own tracking codes.

240. Merchants (and affiliate networks) restrict Capital One's ability to overwrite the tracking codes directly, because Capital One would not get paid a commission if it performed this overwriting directly. Capital One only gets the commission if it causes the tracking codes to be overwritten through an indirect approach: a forced redirect to another website or a hidden tab opening.

241. In this way, Capital One circumvents the technical restrictions placed on browser extensions to artificially "trick" the consumer's browser and the online merchant's website into replacing the legitimate tracking codes of Plaintiffs and Class members with Capital One's illegitimate tracking codes.

242. The Capital One Shopping extension's cookie-stuffing functionality is not disclosed in the applicable terms of service or privacy policy, or in any information that is disclosed to consumers who install the extension in the ordinary course.

243. As a result of Capital One's unlawful scheme, California Plaintiff and California Subclass members have lost substantial revenue from affiliate commissions that were improperly

diverted to Capital One.

244. California Plaintiff and California Subclass members seek compensatory damages, injunctive relief, and all other legal or equitable relief available under the CDAFA.

245. Because Capital One's conduct is willful and fraudulent, California Plaintiff and California Subclass members seek punitive or exemplary damages, as available under CDAFA. Capital One concealed the material fact that it was diverting affiliate commissions from creators to itself, depriving California Plaintiff and California Subclass members of substantial commissions.

## NINTH CAUSE OF ACTION

### PENNSYLVANIA COMPUTER OFFENSES LAW 18 PA.C.S. § 7611 (ON BEHALF OF PLAINTIFF AHNTOURAGE MEDIA LLC AND THE PENNSYLVANIA SUBCLASS)

246. Plaintiff Ahntourage Media LLC ("Pennsylvania Plaintiff") re-alleges and incorporates by reference all factual allegations above as if fully set forth herein.

247. Under the Pennsylvania Computer Offenses Law, 18 Pa.C.S. § 7611, it is unlawful to:

> (1) access[] or exceed[] authorization to access, alter[], damage[] or destroy[] any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof with the intent to interrupt the normal functioning of a person or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;
>
> (2) intentionally and without authorization access[] or exceed[] authorization to access, alter[], interfere[] with the operation of, damage[] or destroy[] any

> computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof . . .

248. Capital One has deployed its browser extension to knowingly access and without permission alter, damage, delete, and/or destroy the tracking codes of Pennsylvania Plaintiff and Pennsylvania Subclass members, by diverting the affiliate commissions that rightfully belong to Pennsylvania Plaintiff and Pennsylvania Subclass members.

249. Capital One has deployed its browser extension to knowingly access and without permission add, alter, damage, delete, and/or destroy the tracking code data of Pennsylvania Plaintiff and Pennsylvania Subclass members, which resides on covered computer systems.

250. Pennsylvania Plaintiff and Pennsylvania Subclass members have an ownership interest in the tracking code data that the Capital One Shopping extension has unlawfully modified, damaged, and/or destroyed. The extension is programmed with computer instructions that are designed to access, modify, damage, and/or destroy the tracking code data of Pennsylvania Plaintiff and Pennsylvania Subclass members without their authorization, in direction violation of the Pennsylvania Computer Offenses Law.

251. Capital One did not request or receive permission from either the consumers of its browser extension or Pennsylvania Plaintiff and Pennsylvania Subclass members to add, alter, damage, delete, or destroy the tracking code data of Pennsylvania Plaintiff and Pennsylvania Subclass members residing on consumers' browsers, nor did Capital One request or receive permission to divert the affiliate commissions of Pennsylvania Plaintiff and Pennsylvania Subclass members to Capital One. Consumers of Capital One Shopping did not grant Capital One access that is necessary to be able to alter tracking codes because consumers themselves do not have that

access and cannot overwrite tracking codes. From a browser's settings, an ordinary computer owner can see the fact that tracking codes are installed and can delete them. But an ordinary computer owner cannot access and overwrite them. One would need specialized "developer tools" or other specialized software to access and overwrite tracking codes.

252. Instead, Capital One circumvented technical barriers that are in place to restrict access and alteration of tracking code data. As described above, when a consumer activates the Capital One Shopping extension, Capital One extension's code surreptitiously injects a new, hidden browser tab in the background to avoid detection by the consumer. This hidden tab redirects the consumer's browser to a purpose-built URL. Capital One then artificially mimics a genuine click on an affiliate marketing link associated with its own affiliate marketing account in this hidden browser tab, causing the online merchant's website to replace the tracking codes of Pennsylvania Plaintiff and Pennsylvania Subclass members with Capital One's tracking codes.

253. Merchants (and affiliate networks) restrict Capital One's ability to overwrite the tracking codes directly, because Capital One would not get paid a commission if it did so. Capital One only gets the commission if it causes the tracking code to be overwritten through a forced redirect to another website or a hidden tab opening.

254. In this way, Capital One circumvents the technical restrictions placed on browser extensions to artificially "trick" the consumer's browser and the online merchant's website into replacing the legitimate tracking codes of Pennsylvania Plaintiff and Pennsylvania Subclass members with Capital One's illegitimate tracking codes.

255. The Capital One Shopping extension's cookie-stuffing capability is not disclosed in the applicable terms of service or privacy policy, or in any information provided to consumers in the ordinary course of installing the extension.

256. As a direct result of Capital One's unlawful scheme, Pennsylvania Plaintiff and Pennsylvania Subclass members have suffered significant financial losses, including substantial revenue from commissions that were improperly diverted to Capital One.

257. Pennsylvania Plaintiff and Pennsylvania Subclass members seek compensatory damages, injunctive relief, and all other legal or equitable relief available under the Pennsylvania Computer Offenses Law.

258. Because Capital One's conduct is willful and deceitful, Pennsylvania Plaintiff and Pennsylvania Subclass members seek punitive or exemplary damages, as available under the Pennsylvania Computer Offenses Law. Capital One concealed the material fact that it was diverting affiliate commissions from creators to itself, depriving Pennsylvania Plaintiff and Pennsylvania Subclass members of substantial commissions.

## VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request that the Court:

A. Certify this case as a class action, and appoint Plaintiffs as Class Representatives and appoint Class Counsel;

B. Enter judgment in favor of Plaintiffs and the Class;

C. Enter injunctive and declaratory relief as is necessary to protect the interests of Plaintiffs and the Class, including to prevent the Capital One Shopping browser extension from taking credit for sales it did not originate;

D. Award all actual, general, special, incidental, nominal, statutory, treble, punitive, liquidated, and consequential damages and restitution to which Plaintiffs and the Class are entitled;

E. Award disgorgement of monies obtained through and as a result of the wrongful conduct alleged herein;

F. Award Plaintiffs and the Class pre- and post-judgment interest as provided by law;

G. Enter such other orders as may be necessary to restore to Plaintiffs and the Class any money and property acquired by Capital One through its wrongful conduct;

H. Award Plaintiffs and the Class reasonable litigation expenses and attorneys' fees as permitted by law; and

I. Award such other and further relief as the Court deems necessary and appropriate.

## IX. JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all issues triable as of right.

DATED: March 25, 2025

Respectfully submitted,

/s/_____

Steven T. Webster (VSB No. 31975)
**WEBSTER BOOK LLP**
2300 Wilson Blvd., Suite 728
Arlington, VA 22201
Telephone: (888) 987-9991
swebster@websterbook.com

*Plaintiffs' Local Counsel*

Norman E. Siegel (admitted *pro hac vice*)
Barrett J. Vahle (admitted *pro hac vice*)
Joy D. Merklen (admitted *pro hac vice*)
**STUEVE SIEGEL HANSON LLP**
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
merklen@stuevesiegel.com

E. Michelle Drake (admitted *pro hac vice*)
Marika K. O'Connor Grant (admitted *pro hac vice*)
**BERGER MONTAGUE PC**
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
T. 612.594.5999
F. 612.584.4470
emdrake@bm.net
moconnorgrant@bm.net

Sophia M. Rios (admitted *pro hac vice*)
**BERGER MONTAGUE PC**
8241 La Mesa Blvd., Suite A
La Mesa, CA 91942
T. 619.489.0300
srios@bm.net

Steven J. Toll, VSB No. 15300
Douglas J. McNamara (admitted *pro hac vice*)
Karina G. Puttieva (admitted *pro hac vice*)
**COHEN MILSTEIN SELLERS & TOLL PLLC**
1100 New York Ave. NW, 8th Floor
Washington, DC 20005

Telephone: (202) 408-4600
Facsimile: (202) 408-4699
dmcnamara@cohenmilstein.com
kputtieva@cohenmilstein.com

James J. Pizzirusso (admitted *pro hac vice*)
Amanda V. Boltax (admitted *pro hac vice*)
Ian E. Engdahl (admitted *pro hac vice*)
**HAUSFELD LLP**
888 16th Street N.W., Suite 300
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com
iengdahl@hausfeld.com

Steven M. Nathan (admitted *pro hac vice*)
**HAUSFELD LLP**
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com

*Plaintiffs' Co-Lead Counsel*

Josh Sanford (*pro hac vice* forthcoming)
Arkansas Bar No. 2001037
Jarrett Ellzey (admitted *pro hac vice*)
Texas Bar No. 24040864
Leigh S. Montgomery (admitted *pro hac vice*)
Texas Bar No. 24052214
Tom Kherkher (*pro hac vice* forthcoming)
Texas Bar No. 24113389
**EKSM, LLP**
4200 Montrose Blvd., Ste. 200
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455
jsanford@eksm.com
jellzey@eksm.com
lmontgomery@eksm.com
tkherkher@eksm.com
service@eksm.com (service only)

Devin J. Stone (*pro hac vice* forthcoming)

**EAGLE TEAM LLP**
Washington Bar No. 260326
1050 Connecticut Ave. NW, Suite 5038
Washington, DC 20036
Phone: (833) 507-8326
devin@eagleteam.law

*Additional Counsel for Plaintiff Ahntourage Media LLC*

Thomas E. Loeser (admitted *pro hac vice*)
Karin B. Swope (admitted *pro hac vice*)
Vara Lyons (*pro hac vice* forthcoming)
**COTCHETT, PITRE & MCCARTHY, LLP**
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Telephone: (206)-802-1272
Facsimile: (206)-299-4184
tloeser@cpmlegal.com
kswope@cpmlegal.com
vlyons@cpmlegal.com

*Additional Counsel for Plaintiff Just Josh, Inc.*

Julian Hammond (admitted *pro hac vice*)
Polina Brandler (admitted *pro hac vice*)
Ari Cherniak (admitted *pro hac vice*)
**HAMMONDLAW, P.C.**
1201 Pacific Ave, 6th Floor
Tacoma, WA 98402
Telephone: (310) 601-6766
Facsimile: (310) 295-2385
jhammond@hammondlawpc.com
pbrandler@hammondlawpc.com
acherniak@hammondlawpc.com

*Additional Counsel for Plaintiff TechSource Official*